# DESIGN AND APPLICATIONS OF SCENARIO-BASED MACHINE LEARNING MODELS

CHEN LERAN

PhD

The Hong Kong Polytechnic University

2025

The Hong Kong Polytechnic University
Department of Industrial and Systems Engineering

# Design and Applications of Scenario-Based Machine Learning Models

CHEN Leran

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy

August 2024

## CERTIFICATE OF ORIGINALITY

I hereby declare that this thesis is my own work and that, to the best of my knowledge and belief, it reproduces no material previously published or written, nor material that has been accepted for the award of any other degree or diploma, except where due acknowledgement has been made in the text.

_____(Signed)

Leran CHEN (Name of Student)

# ABSTRACT

Since the onset of the Fourth Industrial Revolution, human civilization has accelerated towards a new era defined by digitization and artificial intelligence. In various domains such as industrial production, healthcare, and finance, data has been extensively utilized and generated. The development of technologies like the Internet of Things (IoT) and mobile internet has driven the mass creation and accumulation of rich data. The rapid advancement of machine learning has unlocked even greater value from data; the synergy of algorithms and data has propelled innovation and transformation across numerous industries.

In the broad application of machine learning across various domains, several core challenges and limitations persist. (1) The improvement in accuracy relies on complex algorithms and large datasets, making it challenging to balance efficiency and often overlooking the performance of individual object. (2) The advancement of computing power lags behind the rapid generation of data, limiting the full utilization of available data. (3) Low interpretability and customization hinder user acceptance. These issues restrict the broader application and integration of machine learning technologies.

To address the above challenges, this thesis analyzes an observation that models emphasizing generalizability often face difficulties in balancing various performance metrics within specific applications. This research critically examines the conventional emphasis on generalization ability within the existing "Impossible Trinity" of machine learning, i.e. generalizability, efficiency, and accuracy. A framework based on scenario customization is proposed, shifting the focus from generalizability to adaptability and customization while simultaneously pursuing both efficiency and accuracy. The key contributions of this work are as follows:

**Machine learning models tailored to a single individual object.** This approach focuses on the individualized analysis of each object within the scenario to achieve customization for specific scenarios. Subsequent experiments conducted on a Hepatitis C dataset demonstrate that the customized approach achieved an accuracy of 99.49%, surpassing general-purpose algorithms by 5%.

**Machine learning models based on the specific requirements of the application scenario.** This effort primarily aims to achieve optimal results in scenarios by balancing multiple objective functions based on the specific requirements of the scenario. This effort integrates customization for individual people and considers the constraints of actual scenarios. Simulations on the UCI heart disease dataset, mimicking situations of large-

scale screening, achieved an accuracy of 97%, proving the efficacy in model lightweight, privacy protection, and model updates with efficient data utilization.

**Machine learning models inspired by core characteristic of special scenarios.** This approach, through a thorough understanding of actual usage scenarios, identifies and fully leverages the core characteristic of scenarios to simplify problems fundamentally and enhance model performance. In the application of obstacle detection in high-speed railway scenarios, images experiments conducted in the Carla simulation environment showed that detection accuracy improved by 10%, and detection speed increased by up to 75%. With point cloud data, the system achieved unparalleled performance with matching accuracy exceeding 96% and speeds of 116 frames per second.

In conclusion, this thesis advances improved machine learning performance by addressing model efficiency, accuracy, and adaptability with scenario-specific solutions. These innovations enrich both the theoretical and practical aspects of the field, promising more personalized and efficient future applications.

# PUBLICATIONS ARISING FROM THE THESIS

**Chen, L**., Ji, P., Ma, Y., Rong, Y., & Ren, J. (2024). Customized obstacle detection system for High-Speed Railways: A novel approach toward intelligent rail transportation. *Advanced Engineering Informatics*, 62, 102911.

**Chen, L**., Ji, P., Ma, Y., Rong, Y., & Ren, J. (2023). Custom machine learning algorithm for large-scale disease screening-taking heart disease data as an example. *Artificial Intelligence in Medicine*, *146*, 102688.

**Chen, L**., Ji, P., & Ma, Y. (2022). Machine Learning Model for Hepatitis C Diagnosis Customized to Each Patient. *IEEE Access*, *10*, 106655-106672.

# ACKNOWLEDGEMENTS

I am deeply grateful to all the individuals who have supported and guided me throughout my Ph.D. journey.

Firstly, I extend my heartfelt thanks to Professor RONG Yiming, my undergraduate supervisor at Southern University of Science and Technology (SUSTech). Professor RONG has been a pivotal figure in my academic career, offering me invaluable opportunities and recommending me for the collaborative Ph.D. training programme with Hong Kong Polytechnic University (PolyU). His encouragement and belief in my potential set the foundation for my continued academic pursuits.

At PolyU, I was fortunate to have Professor JI Ping as my supervisor during the initial two years of my doctoral studies. Professor JI's passion for research and his dedication to practical and meaningful work deeply influenced me. Our frequent discussions and hiking trips were not only intellectually stimulating but also inspiring. His enthusiasm for new ideas was infectious, and his insistence on conducting research with real-world applications shaped my approach to my studies.

Upon returning to SUSTech for the latter part of my Ph.D., I had the privilege of working under the guidance of Professor MA Yongsheng. From Professor MA, I learned the importance of being a well-rounded researcher. He taught me the value of efficient teamwork, resourcefulness, and the importance of seeking diverse resources. His support and the freedom he provided in choosing research directions and accessing resources were invaluable, and I am deeply appreciative of the opportunities he provided.

During this period, Professor REN Jingzheng at PolyU also became my supervisor. His guidance and insights were crucial in the final stages of my research, and I am thankful for his support.

I would also like to express my sincere gratitude to my family for their unwavering support. Their encouragement and understanding allowed me to focus on my studies without any concerns.

Additionally, I am thankful to all the fellow students, both seniors and juniors, who collaborated with me on various projects and discussions. Their camaraderie and shared efforts were essential in navigating the challenges of this academic journey.

Transitioning directly from undergraduate studies to a Ph.D. program was a path filled with challenges, exploration, and novelty. It is through the collective support and guidance

of the above remarkable individuals that I have reached this milestone. I hope to live up to their expectations and continue to contribute valuable work in the future meaningfully.

Thank you all.

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# CHAPTER 1 INTRODUCTION

Nowadays, data, known as the “oil of the information age” in industry, has been rapidly collected and then widely used in various decision-making tasks. In such processes, machine learning plays an indelible role; in return, data also drives the progress of machine learning. However, due to the lack of synchronization in their development trends between the two domains, the application of machine learning in many specific areas is still limited. In order to enable unique applications of machine learning in specific scenarios, this thesis proposes a scenario-based machine-learning model.

This chapter introduces the background information of the PhD project first with the relevant machine learning models to be investigated in this research. Then, the problem description and specific objectives are elaborated to illustrate the motivation and significance. Lastly, the structure of the thesis is described to display an overview.

## 1.1 Background

In recent years, with the significant increase of computing power and the accumulation of huge data in the industry, the development direction of artificial intelligence (AI) algorithms and applications has mainly followed an approach of training a universal model through synthesizing complex models and massive data (Emmert-Streib, Yang, Feng, Tripathi, & Dehmer, 2020) namely universal AI approach. This approach has indeed produced many excellent algorithms in many fields and a large number of applications in practical scenarios. For example, in prediction and computer natural language processing, the birth of the Transformer (Vaswani et al., 2017b) makes prediction and translation more accurate. In applying the translation of English-to-German and English-to-French, the overall prediction accuracy can get a BLEU (Michael I. Jordan & Mitchell, 2015) score of 35.1. In the computer vision (CV) direction, ResNet (K. He, Zhang, Ren, & Sun, 2016) and the iterative Yolo model (Tian et al., 2019) have been used in various scenarios and solved many object detection problems.

However, these solutions require complex models and large amounts of data, hence have some obvious drawbacks. (1) When training model parameters, complex

models rely on a large amount of data accumulation and need to consume a lot of computing power. To make full use of hundreds of millions of Terabytes (TB) of data and to fully mine the rules reflected in the data, some pre-training models have reached tens of billions of parameters. Although lightweight networks like MobileNet (A. G. Howard et al., 2017) have focused on mobile or embedded devices, the number of parameters of the model and the amount of computation required are still huge. (2) At the same time, the universal AI approach ignores the differences in the world and tries to get the optimal global solution suitable for all scenarios by increasing the number of samples. Such solution models of stacking networks on top of each other seem naive to the real-world complexity. When these vast models are used in practical engineering projects, these models can perform well in most problems after training, but the running speed is unsatisfactory. Too many various parameters make the calculation efficiency of a single problem too low. At the same time, because a vast model has too many levels and countless nodes, it cannot correspond to those features that can be understood by human beings or recognized conceptually in real life, leading to the weak explicability of the model.

Because so far general-purpose machine learning algorithms showed some promising application results, then scenario-based machine learning models, special problem-solving algorithms, and algorithm optimization are relatively ignored. At present, to obtain a specific AI solution in the industry, engineers are to develop and train those deep learning models developed by large companies who published their well-trained models on open-source website. When engineers apply those relevant pre-trained models or algorithms, they can perform some fine-tuning work to make a new one applicable to their specific problem. Such fine-tuning can help on the model's applicability even when the target dataset is much smaller than the original source dataset. However, such a solution still requires further tuning the pre-trained model with a large number of parameters, which requires the user's equipment to be able to carry out large amount of computation. Alternatively, the engineers may choose to process the data directly with the pre-trained model, which eliminates the need for model fine-tuning but also results in the inability to derive optimal results for a specific problem. After the general-purpose model is deployed to a specific usage scenario, there will be too much uncertainty for some specific problems and it is easy to lower the accuracy of the overall machine-learning model. Usually, such uncertainty for a

sample in a classification problem is predicted to be significant, i.e. the accuracy of Top-1 is low. Top-1 accuracy is a metric used to evaluate the performance of classification models, representing the percentage of instances where the highest confidence prediction made by the model is exactly the correct class.

According to industry statistics (United Nations Industrial Development Organization, 2021), thousands of companies around the world need personalized and scenario-based AI models. If existing universal machine learning algorithms are used, model training will bring substantial financial and time costs. There is a desire for scenario-based AI models that are easy to use for end users.

At the same time, in recent years, the issue of data privacy protection (Binjubeir, Ahmed, Ismail, Sadiq, & Khan, 2019; D. Chen & Zhao, 2012; Isaak & Hanna, 2018) has gradually come into the public's view. The current user data is mainly saved and used by the operator. The operator trains the company's analysis model based on the user data, analyzes the user with the model obtained from the training, and then pushes custom content to the user. Many Internet users do not want to submit their private information to operators for processing. However, without their own AI models, users have to raise their data to the operators for processing to get more personalized and custom services. If every user can train and update its own machine learning model on their own personal device, it will significantly help users protect their privacy.

## 1.2 "Impossible Trinity" of Machine Learning

This thesis critically examines the tripartite goals of machine learning, as defined by the current technological landscape: generalizability (generalization ability), efficiency (speed), and accuracy (precision). If these three goals were expressed in adjectives, they would be: general-purpose, lightweight (fast), and accurate. Echoing the economic principle of the "Impossible Trinity," which posits that a country cannot simultaneously achieve a fixed exchange rate, free capital mobility, and an independent monetary policy, this thesis contends that it is equally unfeasible to fulfill all the three objectives in machine learning concurrently (Agarwal, 2020, 2021; Bottou & Bousquet, 2007; H. Zhao et al., 2022). The inherent trade-offs between these goals stem from practical constraints in computational resources, algorithmic complexity, and data diversity (Bhatia, Varakantham, & Kumar, 2019; Caton & Haas, 2024; Cortes,

Mohri, Gonzalvo, & Storcheus, 2020; Y. Jin, 2007; Karl et al., 2023; Morik, Rahnenführer, & Wietfeld, 2023; Schultheis & Babbar, 2022; Sener & Koltun, 2018; K. Singh, Shah, & Vickers, 2023).

An in-depth analysis reveals why these three objectives are mutually exclusive. Generalizability requires models to perform well across diverse and unseen datasets, often necessitating complex and computationally intensive algorithms (Blanchard, 2024; Chatterjee & Zielinski, 2022; Kotsiantis, Zaharakis, & Pintelas, 2006; Malik, 2020). On the other hand, efficiency demands lightweight models that make quick predictions, which can compromise their accuracy and depth. Precision focuses on achieving high correctness and minimal error, which typically increases the computational burden and limits the model's speed. Consequently, most researchers and enterprises prioritize generalizability in the development of algorithms and model architectures, thus facing a critical decision between speed and precision (Briand, Bianculli, Nejati, Pastore, & Sabetzadeh, 2017; Gohil et al., 2024; Nay & Strandburg, 2021; Yao, 2024).

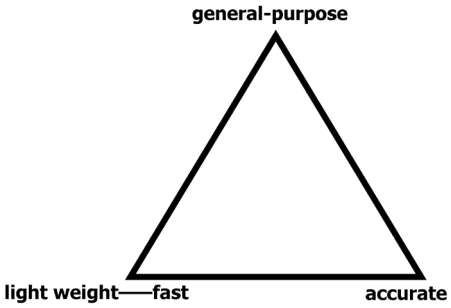



*Figure 1. Impossible Trinity of Machine Learning*

To elucidate this trilemma, consider the following two simplified scenarios for analysis and illustration. These examples illustrate the practical challenges of balancing efficiency and accuracy in machine learning, especially when prioritizing generalizability (Bertolini, Mezzogori, Neroni, & Zammori, 2021; Brodley, Rebbapragada, Small, & Wallace, 2012; Fischer et al., 2020; Lwakatare, Raj, Crnkovic, Bosch, & Olsson, 2020; Rudin et al., 2022; Súkeník & Lampert, 2022). This highlights the complex trade-offs involved in aligning machine learning goals with strategic objectives.

### 1.2.1 The Choice of "General-Purpose" and "Lightweight (Fast)" - Autonomous Driving

Autonomous vehicles need to use machine learning to distinguish among things in a road scene and then guide the control system to drive the vehicle based on the results. Because of the large amount of information contained in the traffic scenario, the types of things that need to be recognized for an autonomous driving recognition system are diverse (Gaurav & Prof; Jeongmin, Sung-Ho, & H; Katona & Bucz; G. A. M, K, & S; G. A. M, K, & S; Majd, Maram, & R; Mohsen, Nima, Michael, & S; Teichman & Thrun). In general, buildings, lanes, other motor vehicles, non-motorized vehicles, pedestrians, signals, road signs, etc. are recognized. In other words, the model is a general-purpose one distinguishing between multiple things rather than a specialized one recognizing only one thing.

At the same time, since autonomous vehicles need to change their driving strategies in real-time in response to external changes in the rapidly changing road scenario, the time taken by the autonomous vehicle recognition system to make a judgment must be very short. This high immediacy requirement forces the recognition system to be "lightweight (fast)" (Apostolos, Víctor, G, & D; Bichen, F, Peter, & K; Hengyu et al.; Heo, Jeong, & Kim; A. J & Alexander; C. Ma, Wang, Chen, & Shen; Manuel, Alvaro, & S; Milanese R, T, S, & J; Mohapatra S, S, H, Stefan, & Patrick; Seonyeong, Sungjun, Youngsok, & Hanjun; Shi-Chieh et al.; Soroush & Cong; H. Wei et al.; W. Wei et al.; Won-Seok, Hansaem, Kyungtae, N, & Jong-Chan; Yongxiang, Qianlei, & Xiaolin).

In the road scenario, the vehicle does not require much accuracy in recognizing things. The vehicle only needs to recognize what a vehicle is encountered but not the type of vehicle, and only where a pedestrian is but not who each individual person really is (Adu-Gyamfi, Asare, Sharma, & Titus; Darthy & Britto; Eduardo et al.; Jamie, V, & A; H. M & Bernhard; S. M & M; Z. M, Michael, B, & K; Morgan). So, in the autonomous driving scenario, the goal of "accurate" is a lower priority and less demanding.

### 1.2.2 The Choice of "General-Purpose" and "Accurate" - Recognition for Finance

Face recognition is already used on a large scale in daily life, for example, unlocking mobile phones, e-payment or clocking in at work, which is a quick and pleasant process

(Doctoral Student, Doctoral Student, Doctoral Student, Doctoral Student, & Professor; Lin-lin; Nijgal, George, & Subramanian). There are, however, situations where face recognition is slow and cumbersome, such as finance-related face recognition. In these applications, financial companies require a high-level accuracy in each face recognition procedure, as it results in the transfer of money or the signing of an agreement (Esan, Ngwira, & Osunmakinde; Jenkins & Burton; Ketcham & Fagfae, 2018; Vishnuvardhan & Ravi, 2021). This demanding face recognition requires the user to remove their glasses and hat, and sometimes requires them to turn or nod their head in order to verify that the user is a real person and not a photograph (Choudhury; Cse Assistant Professor; Muhammad, Amir, & Ahmad; Sharif, Afolabi, Zorto, & Elmedany; Ul Ghani, She, Saeed, & Latif; Wójtowicz & Chmielewski, 2020). Sometimes, the display screen even glows in different colors to verify the face in different lighting conditions (Abd Aziz; Bakshi & Gupta; M. D. M. J, Qiang, Trishul, & G; Kittur, Pasha, Joshi, & Kulkarni; Mhou, van der Haar, & Leung; Sepas-Moghaddam, Malhadas, Correia, & Pereira; Wuming Zhang, Zhao, Morvan, & Chen). This is to ensure that the recognition is very "accurate".

At the same time, the face recognition model is still a "general-purpose" model as it is not specifically developed for a single person, but can recognize all people.

As the whole process adds many extra steps to increase the accuracy of the recognition, the model is not designed to be able to complete each recognition in a very short time, which means that the goal of "lightweight (fast)" has to be sacrificed.

Using the above two examples, this section analyzes how and why traditional machine learning models choose between the three goals. In contrast to the choice made by traditional machine learning models, scenario-based machine learning models attempt to achieve both the "lightweight (fast)" and the "accurate" (Hofer, Roland, Schwarz, & Mayrhofer, 2023; Ríos-Sánchez, Costa-da-Silva, Martín-Yuste, & Sánchez-Ávila; Yaswanthram & Sabarish; Zhe et al.). Although still constrained by the framework of the "Impossible Trinity", this is an exploration of a new direction bridging a research gap.

## 1.3 Problem Statement and Objectives

At present, machine learning models based on huge training data sets still occupy a dominant position in the industry and medical care (D. Carvalho & Cruz; Joshi; P.

Bharathi, Ravindra, & R. Kiran). Many factories and medical institutions have carried out targeted fine-tuning for specific applications, i.e. transfer learning, based on general-purpose models (Ebbehoj, Thunbo, Andersen, Glindtvad, & Hulman; Kora et al.; X. Long, David, Sukhwa, & Patricia; Moradi & Groth; K. D. Singh, Saini, & Singh). The main factor that leads to the transfer learning is that those diverse and changeable scenarios have diverse demands on machine learning models. Some scenarios pursue efficiency, some pursue accuracy, and some pursue interpretability. Unfortunately, traditional machine learning models are not flexible enough to be adapted to different needs (S. A; Dalal, Antoine, & A; Alawieh M & D; Alshehhi M & Di; Menik & Ramaswamy; Sudershan, Anurag, Prahaladha, & Yuvraj). The models that have been widely deployed now are the result of comparative selection based on a large number of experiments, which basically only meet the most important requirements (Alessia, D, & M; Andrei, Raoul-Gabriel, & Neil; V. K. R, A, Shravani, S, & Sankalp; Sachchidanand, Naveen, & V; Zezhen & Yaron). When specific requirements change, such as the need is to significantly improve speed and give up certain accuracy requirements, only changing the model parameters cannot achieve the effect, or having to choose to replace another model. The limitation of such general traditional models leads to a small scope of applications of a single model, so they cannot meet the expectation of switching between multiple specific requirements, and hence bring a lot of tedious work for the application in specific scenarios.

***First problem case***

*An automotive factory analyzes surveillance video through machine learning in order to monitor the operations of production lines. Since the overall assembly line is not working fast, the detection speed of one frame per second is sufficient. And because the working state on the assembly line is more complex, the accuracy of the video analysis is put forward as a high requirement. Combining the above requirements, the factory chose the mature faster-RCNN (*Girshick, 2015*) as the backbone network for machine learning.*

*This factory also has a similar need for parts classification, which requires distinguishing between two kinds of parts delivered in mixed packages. This specific classification task is both similar to and different from the previous assembly line condition monitoring. The similarity is that the video signal is analyzed and judged, but the difference is that the speed and accuracy requirements of the two tasks are very different. Part*

*classification requires fast differentiation of two parts on a high-speed moving conveyor belt at tens of frames per second. However, since there are only two parts, it is easier to differentiate them, and the accuracy requirements are relatively lower. Although the two tasks have some similarities, the same faster-RCNN model cannot satisfy the needs of both tasks by modifying only some parameters, and so separate neural networks are trained according to their respective needs. Since using faster-RCNN is difficult to achieve a particularly high detection speed (unless a particularly luxurious resource investment is used, but it is not justified for a simple classification requirement), so a lightweight network like MobileNet is selected to achieve the detection speed requirement.*

*The same factory may have different requirements for different production steps, and choosing a model that can satisfy all requirements will result in a lot of wasted resources. If different machine learning models are selected as the backbone network for different specific scenarios, it will increase the deployment cost and maintenance cost.*

Meanwhile, with the recent rapid development of computer science and related hardware technologies, professional data collection platforms have emerged in various industries, accumulating a large amount of data and making it possible for industrial upgrading to be data-driven. These data are usually large in scale, diverse, and rapidly updated. After investing a lot of money in data collection, data collectors generally have high expectations for the data and want to utilize the collected data for the training of models instantly to help the subsequent decision-making process. This is not an easy task. Unlike the traditional universal model development path with the data collection, data processing, model selection, and training, now the machine-learning model of the user's challenge is how to use the updated data stream collected in real-time, hence to support the current production activities and to improve the efficiency of production and quality.

***Second problem case***

*A hospital, with the consent of a patient, collected and statistically analyzed the patient's laboratory results and combined them with clinical diagnosis records to form a medical dataset. The medical dataset was analyzed by machine learning, and it was expected that the data could be used to better diagnose the patient's condition. Since machine learning can only make judgments by combining previous data, it cannot be inferred completely out of thin air, so whether the trained machine learning model can*

*better diagnose the condition depends on the comprehensiveness of the data. Unfortunately, it is difficult to collect patient data because it is closely related to personal privacy, and it is also difficult to share data among different medical institutions. This has led to the fact that the volume of data sets related to medical diagnosis is not very large today. Therefore, in the case of rare data, the addition of new data for each case will make the machine learning model more accurate, especially for some rare cases, which will expand the richness of the original dataset more effectively. The timeliness of cases is even more critical when dealing with novel diseases. For example, in the early stages of infectious disease, rapid analysis of new cases is of great relevance and can be effective in saving lives. However, traditional machine learning models do not have the ability to process small amounts of new data in a timely manner; they can only collect a certain amount of data and then train the model uniformly.*

*Another very real problem is the reliability of the model. Traditional general-purpose medical diagnosis machine learning models hope to be able to discriminate between various patients. However, in the real world, different forms of the same disease and the patient's condition after the disease onset vary, especially some special patients are obviously different from the common patients for various reasons. But such special cases are very few after all, which leads to the training process of machine learning models for special cases much less frequent than common cases; in other words, the general model is not sensitive to special cases. This drawback is a problem that needs to be tackled very much.*

In addition to the problems described above that cannot be solved by traditional general-purpose machine learning, the development trend of hardware and software in the information technology industry also requires machine learning to be effective toward specific application scenarios. However, the direction and trends in the field of machine learning are influenced by a variety of factors. Traditional deep learning by continuously increasing model parameters is bottlenecked in terms of accuracy improvement, and so far, the design of lightweight models for use in special scenarios falls into simply using alternative modules with similar effects. New ideas are needed to help break through the bottleneck, both in terms of accuracy improvement and lightweight requirements. In conclusion, alternative types of machine learning models are required in implementation, which need to be fast and accurate, but not too large

and complex to invoke. The evolution of the machine-learning field and the need for lightweight models will be analyzed in more detail in the following literature review chapter.

**Issues to be investigated**

To meet the requirements of future data-driven engineering, this research work proposes four specific issues to be solved. From model perspective, there are:

***Issue 1:*** *How to build a model that can meet the needs of various scenarios by adjusting hyper-parameters?*

***Issue 2:*** *How to create a lightweight but still high-accuracy model?*

From data perspective:

***Issue 3****: How to iterate the machine-learning model quickly in the face of the rapidly updated data?*

***Issue 4****: How to achieve full utilization of the collected data with a focus?*

In order to address these issues, specific research tasks must be taken.

Related to ***Issue 1****,* tasks identified are:

1. Examine why existing models are limited in their scope of application and analyze how to overcome this problem.

2. Summarize existing hyper-parametric optimization strategies and analyze whether they can serve to extend the range of applicability of the models.

3. Investigate existing models with high applicability and analyze their characteristics to find out why they can meet different needs.

Related to ***Issue 2****,* tasks include:

1. Analyze existing design ideas for lightweight models, focusing on the obvious differences from traditional models.

2. Summarize effective ways of improving accuracy in the development of machine learning models and explore the negative effects of these approaches.

3. Explore how to find the optimal balance between the two criteria of model accuracy

and model complexity (number of parameters) in a reasonable trade-off.

Related to ***Issue 3***, tasks include:

1. Investigate the training time and training consumption of the algorithms and models that are now widely used, and find out how often they should be updated with the data they use.

2. Compare and analyze online and offline learning to explore how new data can be applied to an already trained model in a timely manner.

3. Analyze whether the reduced model training time can meet the real-time data needs of today and in the future.

Further, related to ***Issue 4***, Tasks to be done are:

1. Research the amount of data being produced and the amount of data that can be processed, and have a clear understanding of the data-related needs.

2. Analyze what information has already been used and what information is ignored in the existing data set. Try to supplement the original model with the information that has been overlooked.

3. Explore ways to find more important data in the dataset and apply it in a targeted way according to its importance.

In light of the several issues and specific tasks raised above, the objectives of the project are trifold and summarized as follows:

***1) Use scenarios-related prior knowledge to develop new models and algorithms for some specific problems instead of general-purpose models, which are rarely studied in previous literature. Corresponds to: Issues 1 and 4.***

***2) To improve the accuracy and reliability of the model, based on considering the time and computation power consumed in training. Corresponds to: Issues 2 and 3.***

***3) To apply the newly developed models and algorithms to some real industrial or medical cases.***

## 1.4 Definition of a Scenario

"Scenario" is a term that is both abstract and concrete for people. In this thesis, the "scenario" concept includes both the source domain, i.e. the sample space where the data comes from and the target domain, i.e. the sample space where the model is applied. Where the information in the target domain is primarily utilized based on the information in the target domain, since in most cases the data already contains most of the needed information in the source domain. Additional references to the information in the source domain would have to bring in additional professional help, which is difficult and tedious to do. There is a lot of information in the scenario that is overlooked in the traditional machine learning model construction and training process, and this study is intended to enhance the model with this auxiliary information as much as possible. The scope covered by the scenario is shown in Figure 2.

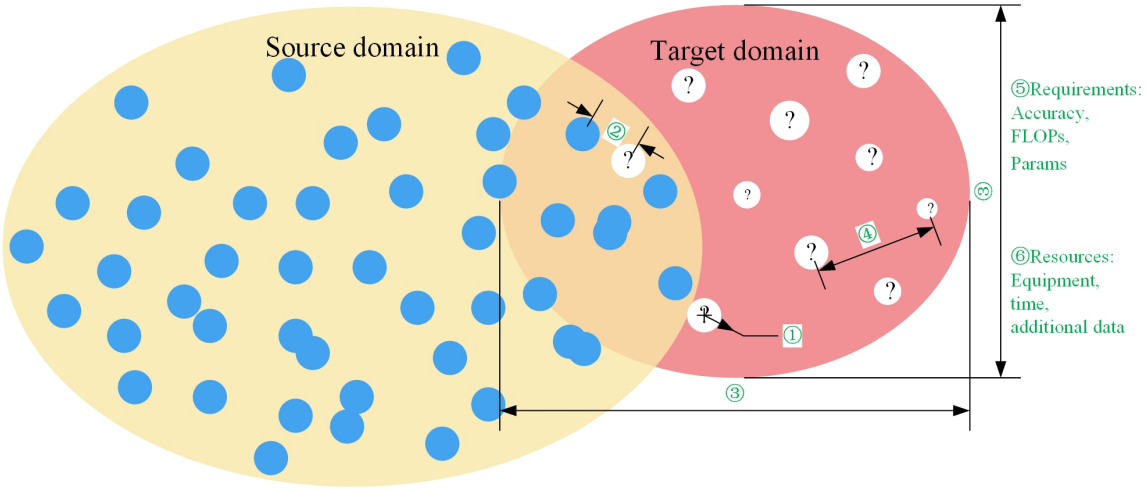



*Figure 2. The scope of the "Scenario".*

Note: Scenarios include source and target domains. In the two domains, the blue circle represents each sample in the source domain (training set), and the white ball with a question mark is the sample to be analyzed in the target domain. In this thesis, the information focused on is shown in green font: ① information about the objects to be analyzed, ② the relationship between the objects to be analyzed and the samples in the training set, ③ the description of the whole target domain and the prior knowledge related to the target domain, ④ the relationships between the objects to be analyzed, ⑤ the requirements of the application scenarios, and ⑥ the resources available in the implementation process.

The information in the scenarios can be basically divided into the following three

categories in addition to the data in the dataset.

1. Information about the object to be analyzed when the model is applied, such as the data of the object to be analyzed, its proportion in the target domain, the proportion of similar samples in the source domain, etc.

2. Additional requirements that the model needs to meet when analyzing, such as the processing speed of each sample, accuracy requirements, limitations on the number of model parameters, preferences for multiple evaluation criteria, etc.

3. The resources that the model can invoke during training, such as the amount of data in the training set, whether additional data are introduced, the hardware equipment used for training, the time constraints during training, etc.

The above is only a brief introduction. In Chapters 4,5,6, different application scenarios correspond to different details. In the beginning part of each of these chapters, the specific scenarios will be analyzed, and then it is made clear how to customize the model according to the specific scenario.

## 1.5 Scenarios and Customization

In essence, this thesis can be succinctly summarized as follows: model customization based on specific scenarios. All scenario analyzes are conducted to achieve better, more appropriate, and more precise customization. Every aspect of customization aims to enhance and excel in serving the specific scenarios. Although the thesis title suggests a focus on “scenario-based” approach, the central theme throughout the thesis is effective and performance-oriented customization.

For the most part, this thesis refers to specialized models as “custom models.” However, the term “customized” is employed when emphasizing the dynamic process of customization, as it conveys the ongoing nature of the customization effort.

## 1.6 Definition of Scenario-Based Machine Learning Models

In the evolving landscape of machine learning, the distinction between scenario-based and non-scenario-based models is pivotal for understanding their applicability, efficiency, and adaptability across diverse domains. This section delineates the precise definitions of scenario-based and non-scenario-based machine learning models,

illustrates non-scenario-based models through concrete examples, and elucidates the inherent drawbacks associated with the latter.

**Scenario-based machine learning models** are specifically designed and tailored to address the unique requirements, constraints, and characteristics of a particular application scenario. Unlike traditional models that aim for broad generalization, scenario-based models prioritize adaptability and customization, ensuring optimal performance within defined contexts. This approach involves: Customization for Individual Objects, Alignment with Application-Specific Requirements, Exploitation of Core Scenario Characteristics.

In contrast, **non-scenario-based machine learning models**—often referred to as general-purpose or generic models—are developed with the intent of broad applicability across multiple domains and use cases. These models emphasize generalization, striving to perform adequately across a wide range of datasets and tasks without significant customization. Common examples include:

Standard Classification Algorithms: Algorithms like Support Vector Machines (SVM), Random Forests, and generic neural networks that are applied uniformly across different datasets without tailoring to specific scenarios. They are difficult to adapt to all scenarios due to the relatively small number of hyperparameters that can be adjusted.

Pre-trained Deep Learning Models: Models such as BERT for natural language processing or ResNet for image recognition, which are designed to handle a variety of tasks but may not excel in specialized applications without further fine-tuning. And if there is a complete disregard for the real situation, using a ResNet with many layers in the pursuit of inference speed or using a lightweight model when very high accuracy is required is a classic example of a model that is not scenario-based.

General Predictive Models in Finance: Models predicting stock prices or credit risks using broad financial indicators without considering industry-specific nuances or individual client profiles. Without considering the requirements of the scenario, rushing to use similar models from other scenarios directly could have serious consequences.

While non-scenario-based models offer flexibility and ease of deployment across

multiple applications, they exhibit several significant drawbacks due to the omission of critical scenario-specific information:

Suboptimal Performance: By not leveraging the unique characteristics of a specific scenario, these models often achieve lower accuracy and efficiency compared to customized counterparts. For example, a generic image classification model may underperform in specialized tasks like medical imaging where specific features are crucial.

Inefficient Resource Utilization: General models may require more computational resources to handle diverse data types and tasks, leading to inefficiencies, especially in resource-constrained environments.

Lack of Interpretability and Customization: Without scenario-specific tuning, these models often lack the interpretability needed for user trust and fail to provide tailored insights, hindering user acceptance and practical utility.

Inadequate Handling of Constraints: Non-scenario-based models typically do not account for application-specific constraints such as privacy regulations, real-time processing requirements, or domain-specific data limitations, limiting their applicability in sensitive or specialized fields.

## 1.7 Potential Applications

In order to better clarify the objectives as well as explain the value of this study, this section presents an analysis of the concrete application effects of scenario-based machine learning models through several real-life comparison cases.

### 1.7.1 Face Recognition Models Tailored to Individuals

The majority of face recognition applications today are for general-purpose, e.g. the most common, simple and fast recognition models for unlocking mobile phones or high accuracy financial related recognition models. These models are suitable for the scenarios where the data provided by a single camera is analyzed and the amount of data to be analyzed is quite limited. However, when it comes to the fast analysis of large amounts of data, most of today's models are not up to the task.

For example, if a terrorist is wanted and the police have some information such as a

photograph of the terrorist. At this point, if a traditional face recognition model is used to analyze the real-time data from a large number of surveillance cameras or to analyze a large number of surveillance videos, it is difficult for a traditional general-purpose face recognition model to do the job. This is because traditional face recognition models need to analyze each person in the video information, identify whom each person is, get a name or an Identity (ID), and then compare this ID or name with the terrorist to determine whether the identified object is the terrorist being sought. Such a cumbersome format is very difficult to implement for very large amounts of video data.

When using a face recognition model that is tailored to the individual, the situation is much simpler. All that needed is to train a model that can only recognize that particular individual based on information collected, such as a photograph of that particular person. Since the model does not need to distinguish between the features of all people, but only needs to be sensitive to specific facial features, the complexity of the model (number of parameters) can be reduced significantly, and the speed of computing is increased. Also, when recognizing faces in a large number of videos, it is no longer necessary to identify which individual each face represents, but only to determine whether it is a correct or wrong face, which simplifies the recognition process. With a face recognition model that is tailored to the individual, it is possible to quickly locate a specific person in a very large amount of video information.

### 1.7.2 Health Monitoring Models Tailored to One Individual

Health is a lifelong pursuit for all people, and it is also the most difficult characteristic to maintain forever. In order to have a healthy body, people need to follow a scientific lifestyle as well as have regular medical check-ups. With the aid of many instruments, the complex indicators of the human body are digitized and standardized one by one. The doctor then uses a large number of statistical data to analyze each patient's indicators for abnormal values, and further consultations are carried out according to the abnormal values. There are some obvious drawbacks to such a program of regular physical examinations to monitor health status: (1) it is a large-scale data-based assessment of individual conditions, which ignores individual differences; (2) it requires the use of many instruments for diagnosis, which is time-consuming, expensive and labor-intensive.

Why is it impossible to overcome these drawbacks? To a large extent, it is limited by

the criterion of “general-purpose”. The human body has many easily measurable indicators that can be collected with simple household equipment. However, as these indicators vary in small amounts and are highly variable between individuals, they cannot be used to monitor the health of a large population.

However, the situation is different when using a health monitoring model that is tailored to the individual. A person’s health can be assessed using data indicators that are more easily collected by the human body. Each individual who wishes to monitor his or her health on an ongoing basis can first test as many indicators as possible with the aid of a variety of instruments to determine his or her comprehensive profile of health. A deliberate week of daily data collection is then carried out. During this week, the healthiest possible lifestyle is adhered to and data is collected at different times of the day. The data that can be collected include: ECG (via smartwatch), blood pressure (portable blood pressure monitor), body fat percentage (body fat scale), visceral fat level (body fat scale), inorganic salt content (body fat scale), etc. All of these data can be recorded by taking quick measurements with simple instruments at home. The data collected for a week of healthy living is then used to form a standard model of personal health. In the future, the standard model of health can be used to assess the state of health, which is very accurate and allows for more frequent monitoring of health conditions. This custom model has several distinct advantages. (1) only one person’s information is recorded, eliminating the need to evaluate unique individuals through a large amount of data from the general population. (2) the model is lightweight (low data requirements) and sensitive (high specificity to the target individual), fully respecting individual differences. (3) The model also eliminates the need to use complex instruments, saving time and money costs. With such a scenario-based model (the actual condition of the individual’s body), the real-time physical health monitoring can be easily carried out.

## 1.8 Structure of the Thesis

With the backdrop of rapid advancements in information technology and data science, this thesis focuses on the performance of machine learning technologies in specific application scenarios. It addresses current issues in machine learning applications first: (1) the asynchronous growth of data and model development, (2) the mismatch between model universality and specific scene requirements, (3)

inefficiency in resource utilization, (4) and insufficient privacy protection. Then, this study proposes a novel approach to machine learning model design tailored for specific scenarios. This scenario-based approach is built on a research strategy that emphasizes customized objectives for individuals, comprehensive consideration of scenario information, and a macroscopic abstraction of the scenario's core. Through an in-depth analysis of the components, lifecycle, and application contexts of machine learning, this thesis establishes a more comprehensive model design and application process. This methodology has been validated for its effectiveness in enhancing model precision and efficiency in real-world medical and industrial cases. This thesis explores machine learning model design oriented towards individual entities, addressing challenges such as data imbalance, inadequate model interpretability, poor adaptability to dynamic environments, and slow model iteration. Customizing models for each patient has resulted in a significant improvement in diagnostic accuracy within specific medical contexts. Furthermore, by introducing a case study of a Custom Obstacle Detection System (CODS), the thesis demonstrates the advanced application and challenges of employing machine learning models in high-speed railway systems, proving the importance and effectiveness of tailoring machine learning models to the core characteristics of specific scenarios.

In summary, this thesis not only enriches the research framework on customized approaches to machine learning issues but also provides theoretical and practical guidance for the application of machine learning technologies in a broader spectrum of fields. The structural framework of this study is illustrated in Figure 3.

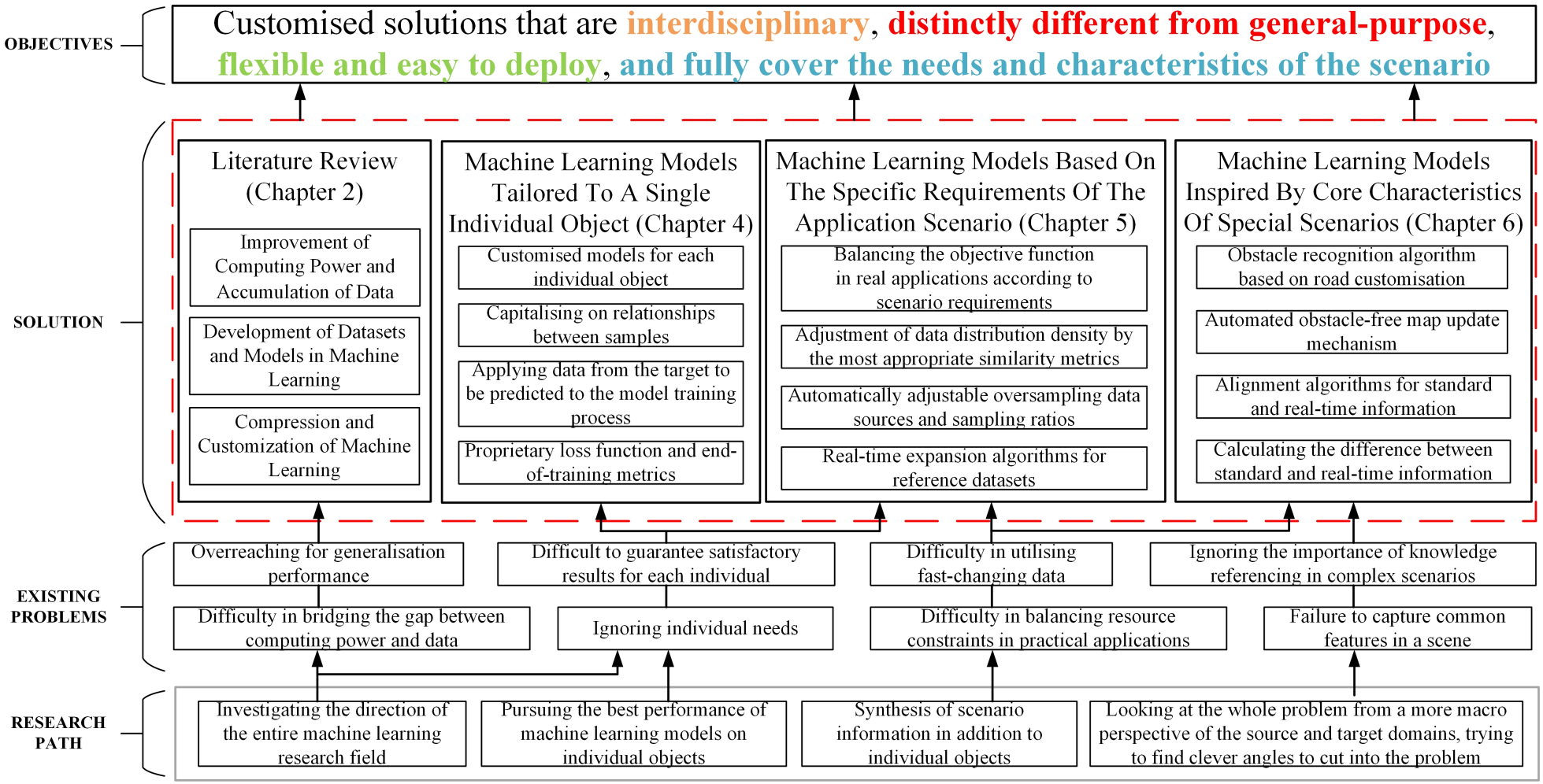



*Figure 3. The framework of the Thesis*

In this doctoral thesis, the development and optimization of machine learning (ML) models for specific scenarios are thoroughly explored, with a focus on the models' customization needs in various application contexts and their impacts on accuracy and computational speed. The text unfolds systematically across seven chapters, ranging from the introduction to the conclusion, encompassing a broad spectrum of research content and methodologies, as well as model design and empirical analysis for individual scenarios.

Chapter 1 Introduction. This chapter outlines the significance of data amidst the swift advancement of information technology, emphasizing the challenges posed by the lack of synchronous development between machine learning and data growth. It introduces the necessity of developing adaptive, resource-efficient, scenario-based ML models tailored for specific contexts. The narrative critiques the prevailing "one-size-fits-all" model approach, advocating for a paradigm shift towards scenario-specific models. This shift acknowledges the "Impossible Trinity" in ML—general-purpose, lightweight, and accuracy—proposing a balanced approach that prioritizes customization over generalization.

Chapter 2 Literature Review. This chapter provides a comprehensive analysis of the directions in which machine learning models are evolving. It discusses the gap between data accumulation and the enhancement of computational capabilities, highlighting the enlightening role of data, computational power, and model integration for ML applications across various domains. The influence of big data and heterogeneous computing on ML development is examined, stressing the importance of customization and simplification in ML, and summarizing the current research limitations.

Chapter 3 Methodology. Detailed descriptions of the research methods employed in this study are provided, including research philosophy, design, ethical considerations, and a summary of the study. The importance of scenario-based data processing, model design, verification, and optimization is particularly emphasized, as well as proposing strategies to reduce model complexity and enhance efficiency for specific problems.

Chapter 4 Machine Learning Models Tailored to A Single Individual Object. This

chapter discusses the limitations of traditional machine learning models and proposes highly custom models to address the variability among individuals, especially in the healthcare sector. The concept and execution strategy of "Machine Learning Models Tailored to A Single Individual Object" are defined and analyzed. The efficacy and accuracy of these tailored models are validated through a Hepatitis C case study.

Chapter 5 Machine Learning Models Based on The Specific Requirements of The Application Scenario. The limitations of traditional models in specific application contexts are discussed, advocating for custom algorithms and models to exploit the uniqueness of domain data, thereby improving model performance and accuracy in real-world settings. The definition of "Machine Learning Models Based on The Specific Requirements of The Application Scenario" is provided, along with an explanation of related concepts and implementation strategies. The advantages of this approach are validated through a large-scale disease screening scenario, with comprehensive experimental evidence showcasing benefits in privacy protection, data updating, and lightweight model design.

Chapter 6 Machine Learning Model Inspired by Special Scenario Core Characteristics. This chapter analyzes how to identify and apply the core characteristics of scenarios. A novel, Customized Obstacle Detection System (CODS) for real-time obstacle detection in high-speed railway systems is introduced, enhancing detection precision and speed in dynamic, complex environments through the integration of real-time sensor data with pre-set unobstructed standard maps.

Chapter 7 Conclusion. The contributions of the entire research are summarized, emphasizing the significance and potential of customizing machine learning models for specific scenarios, particularly in enhancing models' adaptability, accuracy, and efficiency. This offers new insights and directions for future machine learning research and applications.

## 1.9 Summary

This thesis proposes a scenario-based algorithm with the advantages of high accuracy, higher confidence, and fewer resources required to solve unique problems in a particular scenario. Flexible invocations can be made according to the needs of specific issues. It can provide new solutions for tasks requiring high-speed reasoning

in large companies, improve accuracy for specific problems, and make it possible for ordinary people to have their own machine-learning models.

The core idea is to establish targeted machine learning models to specific problems so that the computer “understands” each problem’s focus. Instead of the traditional one-way idea of “data->model->solution”, it becomes “problem->data->model->solution”. In other words, a model is tailored to each specific problem. Since the model does not need to meet the complexity of all scenarios, the overall depth of the model and the number of parameters to be adjusted are greatly reduced. The requirements for training the model can be greatly reduced, and the speed of model inference can be greatly increased.

*Transition Paragraph: Building on the foundational insights from the first chapter on the necessity of scenario-based machine learning models, the second chapter delves deeper into the evolution and current state of machine learning, examining the interplay between algorithmic developments and increased computational power. As we transition from the generalized concepts outlined in Chapter One, the literature review in Chapter Two further emphasizes the imperative for more tailored ML solutions, directly responding to specific industrial and medical needs highlighted previously. This sets the stage for exploring how these specialized models can be strategically developed and applied, ensuring they are both efficient and effective within their designated scenarios.*

# CHAPTER 2 LITERATURE REVIEW

This research is focused on scenario-based machine learning. The necessity of this research comes from three driving factors, as shown in Figure 4.

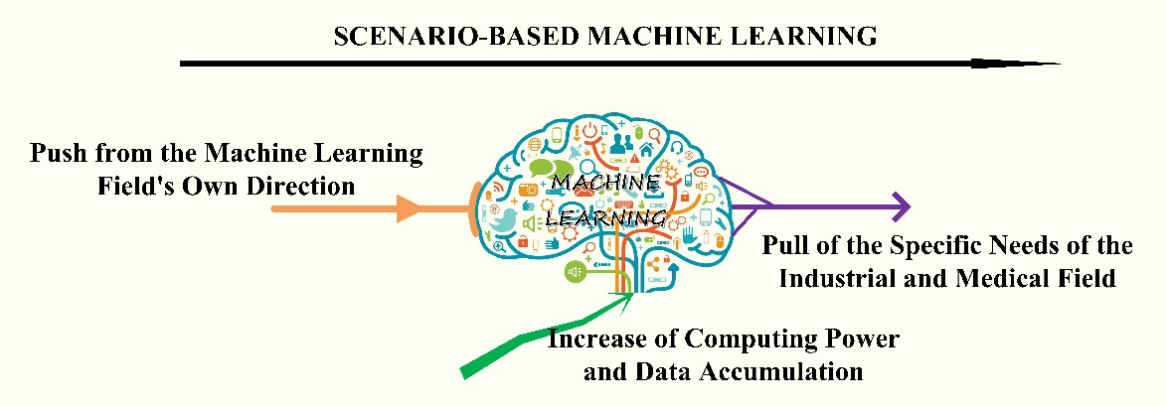



*Figure 4. Motivation and necessity of the study*

The first is the "push" of the machine learning field technology development itself, as described in detail in Sections 2.1.3 and 2.3; the second is the side boost from the increase of computer computing power and data accumulation, as described in detail in Section 2.2; and the third is the pull of the specific requirements of the industrial and medical applications, introduced in detail in Sections 2.4 and 2.5. Section 2.4 primarily discusses the compression and customization of machine learning models, which can be treated as a development approach driven by the specific requirements of the application field.

The literature related to this research work is classified into the following three aspects: (1) the development of machine learning models; (2) the accumulation of data and the improvement of computational power; and (3) the lightweight and customization of machine learning. As the collection of data and the development of computing power determine the application of machine learning in industry and medicine, current and future situations must be analyzed with real-world developments in mind. Therefore, it is beneficial to study the integration of data, computing power, and machine learning models.

## 2.1 Background Knowledge and Development of Machine Learning

As Lao Tzu says in the Tao Te Ching: “It is proper to think of the small and the easy when planning great and difficult things. All the hard things in the world are done from the easy places first; all the big things in the world are done from the small things.” Machine learning is a field with a wide range of research and applications, and it is very difficult to develop an innovative research direction before gaining a deep understanding of the entire field. In other words, it is only after gaining a comprehensive understanding of the development process of the whole field of machine learning and the current hotspots that it becomes clearer to make changes in a specific direction. Therefore, at the beginning of this literature review chapter, a brief summary of the features and developments of machine learning is presented first, and then followed with a view to summarize the future directions of development.

Machine learning is a subdivision of artificial intelligence and a way to achieve equipment intelligence. Machine learning theory is built upon the process of designing and analyzing algorithms that enable computers to “learn” from data by themselves, just like humans. Tom Mitchell (Mitchell, 1997) suggested that “A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P, if its performance at tasks in T, as measured by P, improves with experience E.” The enhanced machine experience can be deemed as exactly what is most widely needed in industry or medicine, that is, to replace or help people making decisions.

With the three industrial revolutions (Heinonen, Karjalainen, & Ruotsalainen, 2015; Rifkin, 2011) that have changed human lives tremendously, many of the dangerous and repetitive mechanized jobs have been solved by automated factories today. If machine learning is used to reduce repetitive human judgment and to improve the accuracy of decision-making, more jobs will no longer require human labor to participate (M. Xu, David, & Kim, 2018). Productivity will be further increased greatly, and hopefully humanity and quality of development as a whole in the world will be improved.

### 2.1.1 Terminology of Machine Learning

After the initial introduction to the definition of machine learning, a brief

description of the terminology related to machine learning covered in this thesis follows hereafter (H. Wang, Lei, Zhang, Zhou, & Peng, 2016). This terminology library focuses on basic concepts and terms in the field of machine learning. The main purpose is to explicate the terminology involved in the thesis for easy subsequent reading. As far as possible, the terms appearing in this thesis are covered. And reference is made to relevant textbooks commonly used in the field (Goodfellow, Bengio, & Courville, 2016; Z.-H. Zhou, 2021).

### ABOUT THE STRUCTURE

**Model:** A *model* is a functional block of data with explicit or implicit defined relations among the elemental data input and output structures maintained dynamically that can achieve a specific function (e.g. mapping) by means of some rules or strategies governing the functions on top of the related data. Its concrete form is a file that contains the processes and parameters for performing operations on a set of data input and generate data output. A *machine learning model* is a model constructed through automated reasoning on top of computer-acquired data input and output relationships.

**Layer: a** *Layer* is the basic type of building block of a machine learning model. Each *layer* is a unit of operation that can perform operations, such as weighting or nonlinear excitation function transformations, on the input data and pass the processed data output to the next layer. A *layer* usually has a fixed function, so it can be simply modularized and compared with the rest of the model. The first and last layers are called "*input layer*" and "*output layer*" respectively, and the middle layers are called "*hidden layers*".

### ABOUT THE STRATEGY

**Learning Algorithm:** An algorithm is a method of generating a model from data, a process.

**Learning/Training:** Obtaining models from the data as required by the algorithm.

**Prediction/Inference:** Using models to obtain outputs based on input information.

### ABOUT THE DATA

**Sample**: Also called **Instance**, a description of an object.

**Training Sample:** Sample that is used for training.

**Testing Sample:** The sample to be predicted.

**Data Set:** An ensemble of data samples.

**Training Set:** A sample dataset for learning, mainly used to train the model. All the input and output information are known and accessible to the model during the training process.

**Validation Set:** The validation set is used to verify and to fine-tune (adjust) the parameters of the learned model, such as the number of hidden units in the neural network. The validation set is also used to determine the structure of the network or to control the parameters of the complexity of the model.

**Test Set:** Tests the discriminative ability of the trained model. The input data from the test set is passed into the model and the model predicts a result and compares it to the output of the test set.

**Feature:** Also known as an **Attribute set**, representing an aspect of an object's characteristics relations, parameters and performance.

**Attribute Values:** Also called **Feature Values**, refers to a feature's parameter values taken by the attributes.

**Attribute Space:** Also known as **Feature Space** and **Sample Space**, refers to the space spanned by feature attributes.

**Distribution:** A law that all samples in the sample space obey.

**Independent and Identically Distributed (i, i, d):** Each sample obtained is independently sampled from this distribution.

**Dimensionality**: Dimensionality describes the number of sample attributes (i.e., the number of dimensions in the sample space).

**Feature Vector:** each point in the attribute space corresponds to a coordinate vector, and each sample can be called a feature vector.

**Label:** Information about the results of the sample.

**Example:** A sample with a label.

**Label Space/Output Space:** The set of all labels.

### About the Task

**Classification:** A prediction process that the predicted result is a discrete value.

**Regression:** A prediction process that the predicted result is a continuous value.

**Binary Classification:** Classification task involving only two classes.

**Multi-Class Classification:** Classification tasks involving multiple classes.

**Positive Class:** The class to be determined in the classification task.

**Negative Class:** A class other than the one to be determined in the classification task.

### Evaluation Criterion

**Underfitting:** A performance description for the model where the model does not capture the data features well, does not fit the data well, and has not learned the general properties of the training sample well.

**Overfitting:** A performance description for the model where the model learns the training sample "too well" and may take some of the training sample's own characteristics as the general properties of all potential samples, resulting in reduced generalization ability.

**Generalization:** The ability of the learned model to be applied to new samples.

**Confusion Matrix:** It is a common tool for evaluating classification problems and is used to record the prediction results of classifiers. In a binary classification problem, the samples can be classified into TP (true positive), FP (false positive), TN (true negative), and FN (false negative) according to the combination of their true and predicted categories.

**Accuracy:** A measure of the model performance description for the model which refers to the ratio of the number of samples with correct predictions (including TP and TN) to the overall number of samples.

**Precision:** The precision rate assesses the accuracy of the model prediction in the positive cases.

**Recall:** From the perspective of actual positive cases, reflects the proportion of

positive samples correctly predicted by the classifier to all positive samples.

**Mean Absolute Error (MAE):** MAE is also known as L1 loss. Although MAE is a good measure of the regression model, the presence of absolute values leads to a function that is not smooth and cannot be derived at certain points. consider changing the absolute value to the square of the residuals, which is the mean squared error.

**Mean Squared Error (MSE):** Mean Squared Error is also known as L2 loss. Since the MSE is not consistent with the magnitude of the target variable, in order to ensure the consistency of the magnitude, it is necessary to square the MSE to obtain the **Root Mean Squared Error (RMSE)**.

**$R^2$ score:** The coefficient of determination reflects the degree of fit of the fitted model to the sample data (Rousson & Gooniu, 2007).

### 2.1.2 Classification of Machine Learning

There are multiple classifications of machine learning that reflect multiple perspectives on understanding machine learning. In this section, the target machine learning domain for this study will be analyzed step by step by introducing different classifications.

#### a) Classification by Learning Form

**Supervised learning.** This type of learning is mainly applicable to regression and classification. This sort of learning allows the computer to learn a specific type of knowledge from a collection of training data, and then predict the results based on the learned knowledge when fresh data arrives. Both inputs and outputs, which may alternatively be defined as features and solutions, must be included in the supervised learning training set. The solutions in the training set are generally collected based on previous facts or labeled by a human. This is a work based on the assumption of regularity and a model more in line with human understanding of the problem and learning knowledge. (Caruana & Niculescu-Mizil, 2006; Cunningham, Cord, & Delany, 2008)

**Unsupervised learning.** Finding the hidden structure directly from the data,

generally without a training process. Some sample data is passed to the computer, and the machine learning algorithm is allowed to analyze this data directly to get some knowledge of the data. For example, determining potential classes (clustering) or changing the form of representation (dimensionality reduction). (Barlow, 1989; Hastie, Tibshirani, & Friedman, 2009)

**Semi-supervised learning.** A learning approach between supervised and unsupervised, usually with the goal of predicting labels as well. (X. Zhu & Goldberg, 2009; X. J. Zhu, 2005)

**Reinforcement learning.** A computer is fed data to learn how to choose a series of actions to maximize the benefit of a particular goal. Reinforcement learning is characterized by trial-and-error interaction with the setting to optimize the decision of action for a sequential decision task. In such tasks, the learning mechanism interacts with the environment by selecting and executing actions that lead to a change in the system state with the possibility of some reinforcement signal (immediate payoff). This type of learning is more like the process of trial and error in a complex and changing environment to find a better strategy. However, it is not suitable for use in industrial and medical scenarios because the direction of changing strategies is disorderly and requires repeated training in a simulated environment, so it will not be explored much in this thesis. (Kaelbling, Littman, & Moore, 1996; Sutton & Barto, 2018)

This thesis covers mainly supervised learning and unsupervised learning, which are more in line with the current needs of the industry where the end user has accumulated some data and wants to play the role of accumulating more and more data.

### b) Classification by learning strategy

The classification approach to machine learning was largely developed very many years ago, but it is still a necessary part of understanding machine learning today. (Carbonell, Michalski, & Mitchell, 1983; Michalski & Kodratoff, 1990)

**Rote learning.** The learner absorbs the information provided by the environment directly without knowledge transformation or any reasoning. The system learns directly by means of a pre-programmed and constructed program, without any reasoning about the input information. This type of machine learning can cover very

limited work scenarios and is not used here.

**Learning from instruction.** The learner takes in the information provided by the surroundings, converts the knowledge into an internally usable representation, and combines the new knowledge with the old knowledge in a structured way. The environment (the source of knowledge) still needs to do a lot of work throughout the process, while the learner's final reasoning process takes a small part. Knowledge distillation techniques are a good illustration of Learning from instruction, taking knowledge from complex models, and subtly teaching it to lightweight models. Knowledge distillation is an effective way to reduce the complexity of a model and will be discussed in more detail later in this thesis.

**Learning by analogy.** Learners use the similarity of knowledge in two different domains to derive the appropriate knowledge in the target domain by analogy from the knowledge in the source domain. Learning by analogy requires more reasoning than **Rote learning** and **Learning from instruction**. In addition, the important transfer learning in machine learning is also based on this strategy. Transfer learning is a technique for retaining the data processing layer of an already trained deep learning network, which will be discussed in more detail later in this thesis.

**Learning by deduction.** The form of reasoning used by students in school in the process of learning knowledge is deductive reasoning. Reasoning leads to conclusions from axioms through logical transformations. This type of reasoning is a process of "fidelity" transformation and specialization that allows students to gain useful knowledge in the reasoning process. The reverse process of deduction learning is inductive learning. This kind of machine learning requires users to have some industry background, which is not conducive to the widespread application of machine learning in the industry and is not discussed here.

**Explanation-based learning (EBL).** Use individual problem-solving examples and construct a causal explanatory structure for the solution process based on domain knowledge and acquiring knowledge. This type of machine learning requires the import of an additional body of knowledge and is not conducive to rapid modeling and analysis of complex matters, and will not be discussed here.

**Inductive learning.** The learner obtains some examples or counterexamples about

a concept from the environment and summarizes the general description of the concept by identifying commonalities among the cases for generalization. This type of learning neither acquires a general description of the concept (e.g., an axiom). Nor is there a similar concept that can be used as a "primitive concept". Inductive learning is the most fundamental and well-established learning method, and is commonly investigated and deployed in the field of artificial intelligence. It is basically the core idea of the model training process, and several inferences and improvement proposals for machine learning models in this thesis are guided by inductive learning ideas.

### c) Classification by application area

**Natural language processing = natural language + machine learning:**

Natural language, unlike computer language, is a kind of information interchange developed during the human development process, including spoken and written language, that represents human thought and is represented in natural language (Chowdhary, 2020). The computer takes natural language input from the user and processes and computes a sequence of internal operations using algorithms designed by humans in order to replicate human understanding of natural language and produce the required results(Hirschberg & Manning, 2015; Nadkarni, Ohno-Machado, & Chapman, 2011).

**Computer vision = machine vision systems + machine learning:**

The image signal from the target will be captured by the image acquisition device and delivered to a particular image processing system, which will convert the image signal into a digital signal based on the pixel distribution, brightness, color, and other characteristics (Voulodimos, Doulamis, Doulamis, & Protopapadakis, 2018). Machine learning takes these digital signals and performs subsequent operations such as finding the target in the picture and identifying it. (Forsyth & Ponce, 2011; Shapiro & Stockman, 2001)

**Robotics = mechanical control + machine learning:**

Traditional robots, such as legged robots that simulate walking, are implemented by methods that rely on hardware platforms and traditional motion control methods. Hardware platforms include high-level hydraulic components and electromechanical

systems, and motion control methods include Quadratic Programming （QP) and Receding Horizon Control (RHC). Boston-Power is the industry-leading benchmark. The current motion control in the lab is usually implemented using machine learning (mainly reinforcement learning), for example, OpenAI has many simulation environments for robot simulation training in its OpenAI Gym for evaluating different reinforcement learning algorithms (Murphy, 2019; Peters, 2007).

**Automatic programming = programming language processing + machine learning:**

A program can also be seen as a computer language, which corresponds to natural language. Automatic programming only requires the user to state his problem without proposing a precise solution algorithm, and machine learning can be applied to better realize this process from "requirement" to "program" at the semantic level (Schmitt, 1989; N. Sharma, Chawla, & Ram, 2020).

**Intelligent search = information indexing algorithm + machine learning:**

Search engines from a generation of simple text indexing, to the second generation of hypertext link-based page rank, and now three generations of applications consider more factors and more comprehensive machine learning (Karwa & Honmane, 2019; Mahesh, 2020).

**Data mining = database + machine learning:**

The use of machine learning methods rather than artificial rules from the database "mining" effective information (Clarke, Fokoue, & Zhang, 2009; Mannila, 1996).

**Expert system = expert-level knowledge + machine learning:**

A portion of expert-level knowledge with high confidence is used as a priori knowledge, combined with machine learning for more accurate reasoning and judgment (Gu, Foster, Shang, & Wei, 2019; Liao, 2005).

Machine learning can be even more powerful when it works together with different bodies of knowledge. In order to allow machine learning to be better integrated with other domains, this thesis will focus on some of the more essential features of machine learning, rather than having too much of a preference for a specific application domain.

### 2.1.3 Development of Machine Learning

The research history of artificial intelligence has a natural and clear lineage from "reasoning" to "knowledge" and then to "learning". The following three paragraphs describe the three periods of AI development.

**Reasoning period.** From the 1950s to the 1970s, it was thought that machines could be intelligent if they were given the ability to reason logically (Minsky, 1961). However, as research progressed, it became clear that logical reasoning alone was not enough to achieve artificial intelligence, and E.A. Feigenbaum and others argued that to make machines intelligent, they had to have knowledge (Feigenbaum, Buchanan, & Lederberg, 1970).

**Knowledge period.** From 1970s to 1980s, during which a large number of expert systems were introduced and made great contributions in many fields (Feigenbaum, 1977, 1979; Minsky, 1974). E.A. Feigenbaum was awarded the Turing Award in 1994 as the father of "knowledge engineering". However, expert systems face a "knowledge engineering bottleneck". Simply put, it is quite difficult for a human to summarize knowledge and then teach it to a computer. So, some scholars thought, how good it would be if the machine could learn knowledge by itself.

**Learning period.** From 1980s to present, machine learning became a separate discipline and began to develop rapidly, and various machine learning techniques blossomed. There were already research works related to machine learning in the 1950s, mainly focusing on connectionist learning based on neural networks with representative works.

The following is a summary of machine learning developments during the learning period. We can conclude from the development process of history that many machine learning ideas are profound. These ideas can show different lights at different stages of development.

When it comes to "learning from examples", (Dietterich & Michalski, 1983) a key effort in the 1980s was symbolic learning, which was represented by using decision trees (Quinlan, 1986, 1987) and logic-based learning (M. C. Chen & Henschen, 1985). As a general rule, decision tree learning is based on information theory and tries to

minimize the entropy of information, directly imitating the tree-like process by which humans make judgments regarding conceptual notions. Inductive Logic Programming (ILP) is a well-known example of logic-based learning (Lavrac & Dzeroski, 1994; Muggleton & De Raedt, 1994), and it may be thought of as the meeting point of machine learning and logic programming. Knowledge representation was accomplished through the use of first-order logic, and induction is accomplished through the modification and expansion of logical expressions. The rise of symbolic learning as the dominant method of learning is inextricably linked to the development of the whole area of artificial intelligence. As previously stated, artificial intelligence progressed through two distinct phases between the 1950s and the 1980s, a "reasoning phase" and a "knowledge phase". People made significant advances in the "reasoning period" based on symbolic knowledge representation and deductive reasoning techniques, whereas in the "knowledge period", people made significant advances based on symbolic knowledge representation and the development of expert systems by acquiring and applying domain "rules". Therefore, from the beginning of the "learning period", symbolic knowledge representation was naturally favored. In fact, machine learning came to the main stage of artificial intelligence in the 1980s as the "key to solving knowledge engineering bottlenecks". Because of their simplicity and accessibility for use, decision tree learning approaches are among the most widely used machine learning techniques today. ILP possesses excellent knowledge representation capabilities and is capable of expressing complicated data connections more readily than other technologies. Furthermore, domain knowledge is generally simply defined by logical expressions, i.e. 'rules', which make it a very useful tool. Consequently, ILP can not only use domain knowledge to support learning, but can also refine and increase domain knowledge as a result of the learning process. However, 'Water can float a boat and sink it as well', as a direct consequence of the overwhelming representation capability, the learning process is faced with too large a hypothesis space and extremely high complexity, and it is difficult to learn effectively when the problem size is slightly large. Research in this area fell into a relative slump after the mid-1990s.

Before the mid-1990s, the other mainstream technique for "learning from examples" was neural network-based connectionist learning. Connectionist learning

made great strides in the 1950s but did not take the lead because many early AI researchers had a particular preference for symbolic representations. For example, Turing Award winner Simon asserted that AI is the study of "symbolic modeling of intelligent behavior", so connectionist research was not included in mainstream AI research at the time (A. Newell & Simon, 1972; Vera & Simon, 1993). In particular, connectionism itself has encountered significant obstacles. As the Turing Award winner M. Minsky showed, neural networks could only be used for linear classification, not even for problems as simple as "exclusive OR" (Minsky, 1961). It was not until 1985 that J. J. Hopfield made significant progress in using neural networks to solve the famous NP problem of the " Traveling salesman problem" that connectionism was brought back into the limelight (Hopfield & Tank, 1985). In 1986, D. E. Rumelhart and others reinvented the famous Back Propagation (BP) algorithm (David E. Rumelhart, Hinton, & Williams, 1986), which had a profound impact(McClelland, Rumelhart, & Hinton, 1986; David E Rumelhart, Hinton, & McClelland, 1986; David E Rumelhart, McClelland, & Group, 1988). Unlike symbolic learning, which produces explicit conceptual representations, connectionist learning produces "black box" models. Thus, from the perspective of knowledge acquisition, connectionist learning techniques have obvious weaknesses. However, the availability of effective algorithms such as BP makes it useful for many real-world problems. In fact, BP has been one of the most widely used machine learning algorithms. The biggest limitation of connectionist learning is its "trial-and-error" nature; its learning process involves a large number of parameters; the setting of which lacks theoretical guidance and relies on manual "tuning". To exaggerate, a single mistake in parameter adjustment can lead to a thousand miles of learning.

In the mid-1990s, "statistical learning" emerged and quickly took over the mainstream stage, represented by Support Vector Machine (SVM) (Cortes & Vapnik, 1995; Joachims, 1998; Vapnik, 1998) and, more generally, "kernel methods". Research in this area began in the 1960s and 1970s, and the foundations of statistical learning theory (Vapnik, 1999a, 1999b) were laid in that period. However, it was not until the mid-1990s that statistical learning started to become mainstream in machine learning. On the one hand, because effective SVM algorithms were only proposed in the early 1990s, their superior performance was not apparent until the mid-1990s in text

classification applications; on the other hand, it was after the limitations of connectionist learning techniques became apparent that people turned their attention to statistical learning techniques supported by statistical learning theory. In fact, statistical learning and connectionist learning are closely related. After SVM became generally accepted, kernel trick was used in almost every corner of machine learning, and kernel methods gradually became one of the basic elements of machine learning.

Interestingly, connectionist learning made a comeback at the beginning of the 21st century and remains the hottest direction in machine learning today. Deep learning, narrowly defined as neural networks with "many layers", came into being. Deep learning techniques have achieved superior performance in several tests and competitions, especially in applications involving complex objects such as language and images. In the past, if machine learning techniques want to achieve good performance in applications, there are high requirements for users. Theoretically, deep learning techniques involve models of such high complexity should have good performance as long as the user's efforts are made to "tune the parameters" and adjust them well. Therefore, although deep learning lacks a rigorous theoretical foundation, it has significantly lowered the threshold for machine learning applicants and brought the technology to engineering practice.

So why is it only getting hot at this point of time? There are two basic reasons: data is abundant and computational power is strong. Machine learning models have a large number of parameters, and if the data sample is small, it is easy to "overfit". Such a complex model, such a large data sample, if the lack of powerful computing equipment, simply cannot be solved. It is precisely because human beings have entered the "big data era" that machine learning technology has sprung to life again.

It is clear from the development of machine learning that many algorithms or techniques that are proven to be effective today were not taken seriously at the beginning. Very often, current research is limited by technology and the limitations of the times, so the academic community cannot accurately judge the actual value of new algorithms, and many questions need time to be tested. From the perspective of development trends, with the development of computer computing power and the accumulation of data, the complex models trained by deep learning algorithms have taken away most of the light in the field of machine learning in recent years. With deep

learning algorithms and huge models in hot demand today, are they free to develop themselves? Or is the development of algorithms and models governed by other factors as well? With these questions in mind, the next section will summarize and analyze in detail the development of computer computing power and the accumulation of data.

## 2.2 Improvement of Computing Power and Accumulation of Data

In recent years, artificial intelligence technology and applications have grown by leaps and bounds, with a large number of powerful capabilities landing in industry and a large number of popular applications in both our lives and our work. Thanks to the three main elements driving the development of artificial intelligence, the key resources of the digital economy era: data, computing power, and algorithms.

Big data is the new means of production, equivalent to the ingredients needed for stir-fry, the computing power is the new productivity, equivalent to the fuel needed for stir-fry, and the machine learning algorithm is the new production relationship, equivalent to the cooking method. These three elements are indispensable, promote and support each other, and are the necessary conditions for intelligent technology to create value and succeed, and constitute the most basic production cornerstone in the era of the digital economy. Since this study wants to make some improvements in the field of machine learning algorithms as well as models, it is necessary to analyze the progress in data as well as computing power.

### 2.2.1 Computing Power

As a result of a new phase of technological revolution and industrial change currently underway, the global economic structure is undergoing transformation. Computing power, as a new productivity in the era of the digital economy, provides a firm foundation for the growth of the digital economy. It contributes significantly to the advancement of science and technology, the facilitation of the digital transformation of industries, and the promotion of economic and social growth (China Academy of Information and Communications Technology (CAICT), 2021b).

### a) Definition and classification of computing power

In a narrow sense, computing power is the computational capacity of a device to achieve a specific result output by processing data. WD. Nordhaus, the 2018 Nobel Laureate in Economics, proposed in his article "The progress of computing(Nordhaus, 2001)" that "Computing power is the amount of information data that a device can process per second according to the change of its internal state". The core of computing power implementation is CPU, GPU, FPGA, ASIC, and other types of computing chips, and is carried by computers, servers, high-performance computing clusters, and various types of intelligent terminals, etc. Massive data processing and various digital applications are inseparable from the processing and calculation of computing power. The larger the value of computing power represents the more comprehensive computing power, the common unit of measurement is the number of floating-point operations per second (Flops) (Smith, 1988). It is estimated that 1 EFlops (1 EFlops = 10^18 Flops) is about 250,000 mainstream two-way servers, or 2 million mainstream notebooks computing power output. FP32 is a single-precision floating-point number, which uses a 32-bit binary to express a number and is commonly used in multimedia and graphics processing calculations. FP16 is a half-precision floating-point number, which uses 16-bit binary to express a number and is suitable for applications in deep learning.

Computing power, in a broad sense, represents the new productivity in the digital economy age, and it serves as a firm basis for the advancement of the digital economy. At this point, the rapid development of 5G, cloud computing, big data, the Internet of Things, artificial intelligence, and other technologies has fueled the explosive growth of data and the increasing complexity of algorithms, resulting in a rapid increase in the demand for computing power on a large scale and a large capacity, respectively. The study of the development with the level of computing power allows the development of algorithmic solutions that match the level of computing power.

Computing power scales are divided into three categories at this point: basic computing power, intelligent computing power, and supercomputing power. These categories give basic general computing, AI computing, scientific engineering computing, and supercomputing power. Basic general computing power is primarily provided by servers with CPU chips. Intelligent computing power is primarily based

on accelerated computing platforms with GPU, FPGA, ASIC, and other chips to provide more resources for artificial intelligence training and reasoning. Supercomputing power is primarily based on the capacity provided by high-performance computing clusters such as backbone supercomputers, among other things.

### b) Current situation and trend of computing power development

The global scale of computing power is increasing. 2020 global total computing power scale has reached 429EFlops, with a growth rate of 39%, of which the scale of basic computing power (FP32) is 313EFlops, the scale of intelligent computing power (converted to FP32) is 107EFlops, and the scale of supercomputing power (converted to FP32) is 9EFlops.

In the last ten years, the number of computer resources available for training artificial intelligence models has increased tenfold, the computational complexity of AI training has increased tenfold every year, and AI computing has emerged as a mainstream type of computing. China's computing power structure has changed too in recent years in response to changes in application demand; the proportion of basic computing declined from 95% in 2016 to 57% in 2020, while the proportion of intelligent computing increased from 3% in 2016 to 41% in 2020. AI complicated models, the processing requirements of complex scenarios, and the demand for AI-oriented computing power infrastructure are all driving the development of intelligent computing centers, which are presently the primary focus of research and development. With the opening of the era of everything perception, everything interconnection, and everything intelligence. According to IDC forecast data, it is estimated that the global computing power scale will grow at a rate of more than 50% in the next five years, and the overall scale will reach 3300EFlops by 2025.

Diversified demand acceleration, computing power diversification upgrade. Cloud computing continues to see tremendous growth and innovation in terms of fundamental processing power, and according to IDC statistics, the worldwide cloud computing market size will reach US$312 billion in 2020, representing a 24.1% year-on-year increase (International Data Corporation (IDC) 2021b). As a result of the digital transformation of the industry, cloud computing technologies are continuing to be used

in companies, resulting in an overall improvement in technical architecture, application effectiveness, and cloud-based advantages.

### c) The breakthrough direction of computing power and the opportunities brought to algorithms

The rate of advancement in processing power has been boosted even more. Moore's Law (Schaller, 1997; Theis & Wong, 2017) is currently slowing down, and the development mode of classical computer systems, which is driven by improved technology upgrades, is being challenged by bottlenecks such as the "power consumption wall" and the "memory wall".

To cope with the incremental demand for computing power supply in the era of intelligence in all things, it is important to explore the potential of computing devices, computing chips, computing systems, computing theories, and other levels of technological growth, and to explore more dimensions and elements of collaborative innovation to support further upgrading of computing power. In the process of computing power development, different forms of computing and the acceleration advantages of different forms of computing for special problems will influence the design tendency of machine learning algorithms and models. *The development of machine learning algorithms should adapt to the trend of computing power development and use the algorithm that can give the fullest play to computing power to solve practical problems.*

**In terms of computing chips, Moore's Law continues.**

With the help of Fin Field-Effect Transistor (FinFET) size miniaturization (Boukortt, Patanè, & Crupi, 2020), design and process co-optimization technology, enclosing the gate nanosheet, high numerical aperture extreme ultraviolet lithography new structure, new equipment, new material support, integrated circuit manufacturing process subsequent upgrade path has become increasingly apparent in recent years. As a result, the chiplet, 2.5D and 3D advanced packaging, and other technologies are being used to achieve different processes, and heterogeneous integration between different types of chips is becoming an important direction to achieving the overall performance of computing chips and systems while maintaining Moore's Law. However, from the growth rate, through advanced technology to make computing

chips per unit area computing power increase, power consumption decline in the progress of the speed is gradually slowing down. *In the future, improving the overall level of computing power on a large scale will be very dependent on the additional space and energy input, which means that if the algorithm needs more computing power will require more money, the algorithm may fall into the stagnation brought about by the lack of computing power at the end of the 20th century. We can no longer continue to rely on super-complex algorithms with huge numbers of parameters.*

**In terms of computing architecture, multi-level heterogeneous computing is gradually gaining popularity.**

Through the mixed collaboration mode of multiple computing units, heterogeneous computing improves computational parallelism and efficiency. As a result, heterogeneous computing has contributed to a significant increase in various typical applications such as mobile Internet, artificial intelligence, and cloud computing. Heterogeneous computing achieves the best balance between performance, power consumption, and cost, primarily through two modes: on-chip heterogeneity and on-node heterogeneity. On-chip heterogeneity is often represented by system-on-a-chip (SoC) devices, such as the Apple M1 chip, which provides performance that is superior to that of general-purpose CPUs by combining CPUs, and graphics processing units (GPUs), neural processing units (NPUs), and other cores. Nowadays, machine learning algorithms in the training process generally use the CPU to pre-process data and implement other functions of the program, while using GPU for model training. The CPU and GPU are working in succession in a continuous cycle. This requires the algorithm to be designed to take into account the applicability of various types of chips, and not to design an algorithm in which the GPU can complete the backpropagation training but the CPU cannot complete the data preprocessing. For example, in the node heterogeneous, storage and computing to improve the overall capacity of the conditions, the algorithm design can break through the original read and write bandwidth limitations, and optimize the relationship between data processing and model training steps to improve the overall training efficiency. *With the help of this particular structure, the training of machine learning models may be possible on more devices than the current popular form of having large companies train models for users to use. This is where models that are light enough to be trained by individual users are*

*essential.*

**From the perspective of computing systems, the construction of computing power infrastructure continues to accelerate.**

It is expected that global supercomputing will enter the era of E-class computing and that the cloud-based service model will be explored in order to provide flexible and elastic computing support. In the future, cloud supercomputing will serve as an important supplement to supercomputing in order to meet the rapidly growing demand for high-performance computing. After the related infrastructure is gradually popularized, the algorithm adaptation for different types of scenarios becomes a very real problem. *Now the more mature machine learning algorithms are developing in the direction of omniscience and omnipotence, and there are still some gaps in the practical application of specific scenarios with their own focus. Therefore, it is crucial to explore the adaptation of algorithms and models for specific scenarios.*

With sufficient research and analysis of the current computer computing power, it is concluded that the development of algorithms should do the following.

Developments in computing power gave machine learning a period of glory, but now things seem to be starting to look different. Machine learning has to take into account the state of development of computing power and use the resources that have been developed wisely. But it is also important to try some new ideas where appropriate, such as moving away from the blind pursuit of general-purpose models and designing and using models through scenario-based thinking.

### 2.2.2 Big Data

At the moment, the globe has entered the era of the digital economy, and governments place a high value on the growth of this sector of the economy. The technology sector and application innovation are continually pushing the envelope to achieve greater heights. Big data improves factor supply by digitizing it, widens organizational boundaries by networking it, and increases output efficiency by incorporating intelligence into it. Besides being an essential area to encourage the development of strong networks in the country, it is also important strategic support for accelerating the quality change, energy efficiency transformation, and powerful

transformation of the real economy in this new era. After years of development, big data is becoming an element, resource, power, and concept integrated into various fields of economic and social development in the emerging technology industry (China Academy of Information and Communications Technology (CAICT), 2021a).

But is this extensive accumulation of big data really being used to its full potential? What changes or adjustments should be made to machine learning models in the face of such rapidly evolving and rapidly accumulating big data? All these questions will be discussed in the following sections.

### a) Definition and classification of Big Data

Big Data is defined as data that has qualities such as a huge volume, a diversified structure, and a high degree of timeliness; it is a collection of data that cannot be acquired, managed, and analyzed within a certain time limit using standard software. In order to make use of new technologies, such as new processing models, new computer architectures, and clever algorithms, it is necessary to first understand what information is. It is a huge, rapidly growing, and diversified information asset that provides greater decision-making power, insight finding, and process optimization capabilities than previously available. With the use of Big Data comes more focus on the application of new concepts to aid in decision-making, the discovery of new information, and the optimization of business processes online in a closed-loop environment.

Big Data, from a conceptual standpoint, opens the door to a new way of thinking about problems. Large-scale data collection and analysis have given rise to new meanings for the term “factuality”, one of which is “data-driven”, which means that business management decisions can be guided by data from the bottom up, or even by machines based on data, as in the case of quantitative stock trading and real-time bidding advertising. The second is “data closed-loop”, and by studying the big data cases in the Internet industry, they have discovered that they are often able to construct a complete “data closed-loop”, which includes data collection, modeling and analysis, effect evaluation, and feedback correction, allowing them to continuously upgrade themselves and spiral upward in the process. Many “big data applications” are currently being developed that are either not large enough or not required to make use

of the latest generation technology, but they reflect the data-driven and data-closed-loop thinking and improve the efficiency of production management, which is a reflection of the application of the concept of big data thinking in the production environment. A byte is a unit of measurement used by computer information technology to measure storage capacity. The amount of information storage is a measure of the number of programs and data stored in memory, and its main unit of measure is bytes.

The most distinguishing attribute of big data is its vastness; the amount of information collected, stored, and computed is enormous. In recent years, as a result of advancements in science and technology, as well as the widespread use of the industrial Internet of Things, the global data volume has increased dramatically in a short period of time, and the standard relational database cannot handle such a large quantity of data. At the same time, big data necessitates a rapid increase in the rate at which data is sent. Data processing efficiency is critical in a world where there is a massive volume of information being generated. The creation, storage, and analysis of large amounts of data must be completed in real-time in order to be effective in today's world of big data. Data types and sources have become increasingly diverse as a result of the increase in data gathering channels in recent years. Structured, semi-structured, and unstructured data are now included, such as web logs, audio, video, and photographs, as well as geographic position information, among other types of information. Because there are so many different forms of data, the ability to process them all raises the bar even higher. The data types can be classified according to the classification as follows: (1) Structured data: Excel files, CSV files, etc. Structured data is data in the form of tables: each column has the same data type and cannot be further subdivided. (2) Semi-structured data. Emails, web pages, JSON files, log files, etc. The structure and content of these data are mixed together and there is no clear distinction. (3) Unstructured data: pictures, videos, etc.

### b) Current situation and trend of computing power development

Following the development of information technology in numerous industries, such as the medical field, transportation, finance, and other disciplines, a large amount of internal data has been amassed, which has been categorized as "big data resources".

In recent years, the development of mobile Internet and the Internet of things has greatly enriched the channels for collecting large amounts of data. Data from external social networks, wearable devices, automobile networking systems, the Internet of Things, and government public information platforms will become the primary source of incremental data resources for big data. How to connect business logic and access data value using sophisticated machine algorithms in an era of vast information but low-value density is the most significant challenge to be solved in the era of big data, and it is also the most difficult topic to master. Based on prediction statistics from IDC, there will be more than 40 billion worldwide Internet of Things (IoT) devices in 2025, creating up to 180 ZB in data volume, with more than half of the data processing requiring terminal or edge computing capacity. It is predicted that worldwide data production and replication would expand at a compound annual growth rate (CAGR) of 23% throughout the projection period, reaching 181 ZB by 2025, according to IDC's latest Global DataSphere Forecast 2021-2025 (International Data Corporation (IDC) 2021a). In short, the rate of data accumulation has become significantly faster than the rate of development of computing power.

### c) The breakthrough direction of big data and the opportunities brought to algorithms

The underlying technological structure of the big data system has, for the most part, reached maturity at this point. It is becoming increasingly clear that big data technology is evolving into a supportive infrastructure, and that its development is shifting away from increasing efficiency and toward a greater emphasis on personalized upper-layer applications. The trend toward technological convergence is becoming increasingly apparent. *This section will present many convergence tendencies in big data technologies, as well as the potential and problems that algorithms present in the process of big data development, among other things.*

**Stream batch integration: the optimal solution for balanced computational cost-effectiveness.**

Stream processing is capable of properly handling information that changes in real-time, allowing it to accurately represent the real-time dynamic changes of information hotspots in real-time. While offline batch processing is better capable of

capturing the cumulative feedback of past data, online batch processing is more efficient. The notion of lambda architecture was created early in the industry to allow the coexistence of batch and stream processing in computing scenarios while taking into consideration of the balance between the need for real-time computing and the availability of computing resources. In line with the evolution of technological architecture, stream-batch integrated computing is becoming a trend, and it is continually progressing toward more real-time and efficient computing in order to serve richer big data processing requirements. The core requirement of stream-batch integration is to be able to handle even changing information, which is the part of traditional machine learning that still needs continuous improvement. The more mature solutions currently rely on the accumulation of large amounts of data and the extraordinarily long model training of complex models, which by the time a usable model is ready for deployment already has a large time lag from the moment of data collection. This also means that there is a certain time scale impact between the training data in this model and the real-time prediction data. In today's world where everything changes rapidly, this time scale gap may bring about an unacceptable final error after the output. Therefore, machine learning algorithms need to keep up with the development trend of big data and make targeted enhancements for real-time information processing problems. *If all the data collected is transmitted as input to the model for analysis and processing in one fell swoop, it is clear that the current computing power is no longer capable of carrying such demands. This requires pre-processing the data and passing the data with focus into the model.*

**TA (Transaction and Analysis) integration: hybrid transaction/analysis to support immediate decision making.**

The integration of the Transaction and Analysis systems is referred to as TA integration. When conventional business applications make technological selections, the matching database technology will be chosen based on the many use situations to be encountered. When the application requires rapid response to a large number of concurrent user actions, the transaction-oriented OLTP (OnLine Analytical Processing) database will be used; when the program requires multidimensional analysis of a big quantity of data, the analysis-oriented OLAP database will be utilized. In today's data-driven refined operation, it is impossible to ignore the need for enormous real-time

data analysis, which is becoming increasingly common. However, from the viewpoint of the objectives of these solutions, the main purpose is to allow high traffic and high-density data to be analyzed and stored in real-time. The training process of machine learning can generally be seen as an analytics-oriented usage scenario, where the use of data tends to be a multi-dimensional analysis of a large amount of data at once. *However, the deployed machine learning model can be seen as a transaction-oriented application, which requires fast data extraction and prediction and output based on highly concurrent user operations. This also requires the design of future machine learning algorithms to fully integrate the characteristics of database TA integration, and choose the appropriate training set size to adapt to the ratio of data extraction rate under database transaction scenarios and analysis scenarios. This also places demands on the model to be able to handle data of all sizes.*

**Module integration: one-stop data capability reuse platform.**

It has been a while since big data tools and technology stacks were developed, and large corporations have gradually built up an infrastructure of capabilities around the production chain of tools and data, data management, and application in real-world experience. The goal is to unify the view and standards of data assets and provide common data processing, management, and analysis capabilities through this concept. It is becoming increasingly common to integrate data capabilities into existing enterprise systems, which brings data and business closer together and enables the use of data-driven choices to be made more quickly than previously possible. The primary goal is to address three issues: first, to increase the efficiency of data collecting; second, to open the channel for data exchange; and third, to give a unified capacity for data development. With the maturity of module integration, the output of machine learning algorithms must also follow the needs of other modules, and not just stick to the traditional fields. *This requires, first of all, that the algorithms should no longer have too many harsh restrictions on the input data, but should process as many kinds and orders of magnitude of data as possible. The models should also be able to do different types of data output for different needs. At the same time module integration also means that the different modules are more closely connected to each other, which further puts a higher demand on the speed of machine learning models to process data again. The slower data processing speed of a huge number of models may be a constraint to the efficiency of the whole process.*

**Cloud-data integration: The trend toward cloudiness lowers the barrier to technology use.**

The movement of big data infrastructure to the cloud is a significant trend in the data center industry. All major cloud suppliers have begun to offer a variety of big data products to fulfill the demands of their customers, and some have even developed their own on-cloud data solutions. Now, more and more big data products are following the notion of cloud-native development from the beginning of their design, being born in the cloud and growing in the cloud, making them more fit for the cloud's ecology of data storage and processing. The most significant benefit of moving to cloud-based solutions is that users no longer have to worry about how to maintain the underlying hardware and network, and can instead concentrate on data and business logic. This reduces the learning curve and uses thresholds associated with big data technology, allowing for greater adoption. Going to the cloud means that the state of data storage and the location of data processing have changed significantly. The change of data storage state will cause the potential of a data leakage caused by the non-localization of data in the cloud. To reduce the potential harm caused by a data breach, many companies choose to mask some important data to be data desensitized. Sometimes the desensitized data can have a significant impact on machine learning, making it extremely difficult to analyze the data. *This is the most realistic test of machine learning algorithms, whether they can analyze effectively from the desensitized data. Another problem posed by storage in the cloud is the issue of the operating environment. Locally deployed machine learning algorithms can call different APIs (Application Programming Interface) in the local environment as needed to simplify the complexity of the program. But the cloud environment is sometimes not so easy to install new software libraries (packages), which requires algorithms to be designed to minimize the dependence on additional external interfaces. Custom scenario-based models allow for interface calls to be made on demand, resulting in significant deployment cost savings compared to generic models.*

After a thorough discussion of the development of computer computing power and big data and future trends, three questions arise: How to solve the speed difference between computing power and data accumulation? How can the rapidly accumulating data serve as a knowledge environment for existing machine learning models to

rapidly iterate? What scale of complex models can be supported by the present data and computing power? The analysis in the next section will address these three issues.

## 2.3 Development of Datasets and Models in Machine Learning

With the rapid accumulation of data, a variety of all-encompassing datasets have been built. These datasets are as important to machine learning as oil is to manufacturing, nourishing the development of machine learning. To better understand the development of these datasets and the current state of the models trained on them, this summary will analyze the development of large datasets and models based on a few very well-known datasets. It also discusses the development of machine learning models in comparison with the development of computing power and data in the context of the previous two sections.

A joint team in its research article (Sevilla et al., 2022), divides the computing power trend of machine learning into three eras as Figure 5: pre-depth learning era, deep learning era, and large-scale era, which nicely sorts out the current computing power evolution pulse. Now machine learning has bought into the large-scale era. a new trend of large-scale models emerged around 2015-2016. This new trend started with AlphaGo at the end of 2015 and has continued until today. As seen from the graph, there are some very classic algorithms that have driven the whole field at different times in the development of machine learning. From the perspective of several similar overview articles, the representative algorithms chosen are relatively consistent. The most recognised datasets behind these algorithms were found in reverse by going through these most famous algorithms. One dataset from each domain is selected as representative for the analysis of the development of this domain.

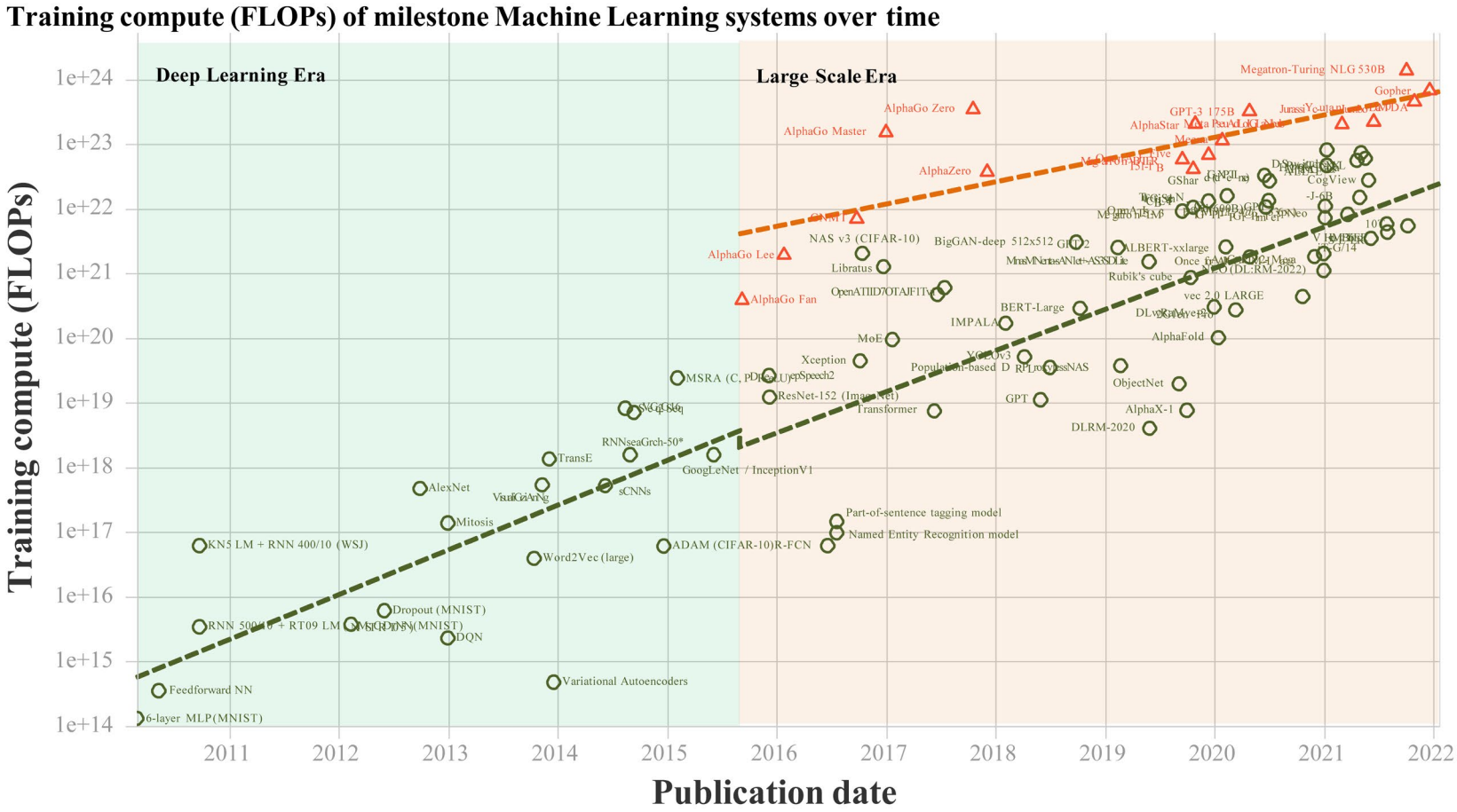



*Figure 5. Training compute (FLOPs) of milestone ML systems over time (Sevilla et al., 2022).*

### 2.3.1 Computer Vision: ImageNet

The ImageNet dataset is a computer vision dataset that was developed under the direction of Professor Feifei Li (J. Deng et al., 2009). The collection contains 14,197,122 photos and 21,841 Synset indexes, which are organized according to the WordNet hierarchical structure. It has been utilized in the ImageNet Large-Scale Visual Recognition Challenge (ILSVRC) since 2010, which is a benchmark for picture categorization and object recognition on a large scale.

The ImageNet dataset is a huge picture dataset that was designed to aid in the development of computer image recognition systems. Each image in the collection has been manually classified with a category, which makes it easier to search for images. The photos in the ImageNet collection represent the majority of the image categories that one might encounter in everyday life. The ImageNet-based image classification problem is a fundamental job in which the goal is to comprehend the complete image as a single unit. The purpose is to categorize photos by assigning them to certain labels in order to achieve classification. Most of the time, image classification is used to refer to the study of photographs of a single item. Object detection, on the other hand, entails tasks like classification, and it is used to assess more realistic circumstances in which many items may be present in a single image.

As shown in Figure 6, 7 and 8, in terms of trends, although the accuracy is still slowly increasing in recent years, the improvement has been very limited. Moreover, the cost in terms of computational effort to achieve a higher level of accuracy is significant. and now looking back at what was once considered the most bloated VGG network (Simonyan & Zisserman, 2014), it looks very “pocket-sized”. There is always a new approach that shines in a year or two, and there is always a newer approach that beats the work of its predecessors and ushers in the new era From the large-scale CNN (Krizhevsky, Sutskever, & Hinton, 2012) in 2012, to the ResNet (K. He et al., 2016) afterward, to the transformer which is now in full bloom in many fields, it can be said that the progress of the model is inseparable from the continuous improvement of computer computing power. *However, even the hottest computer vision in the field of machine learning has slowly entered the bottleneck in recent years and needs to be improved in directions other than accuracy.*

# Image Classification on ImageNet

Leaderboard Dataset

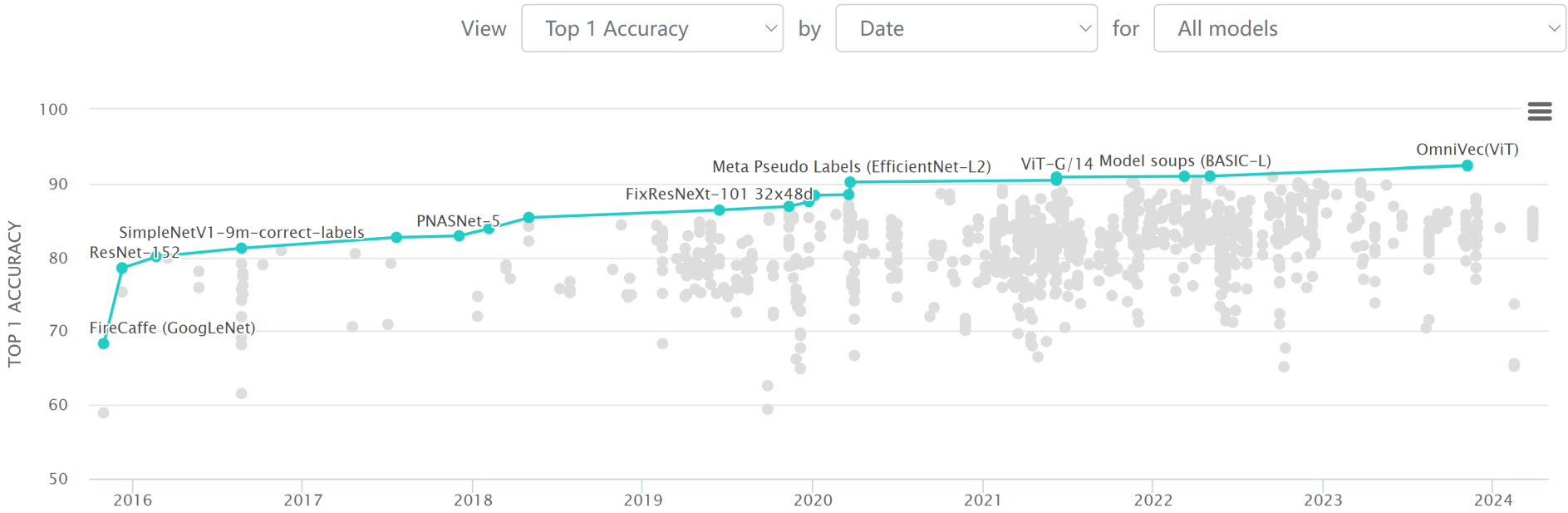



*Figure 6. Top1 accuracy rate on ImageNet for image classification problem (paperswithcode.com)*

# Image Classification on ImageNet

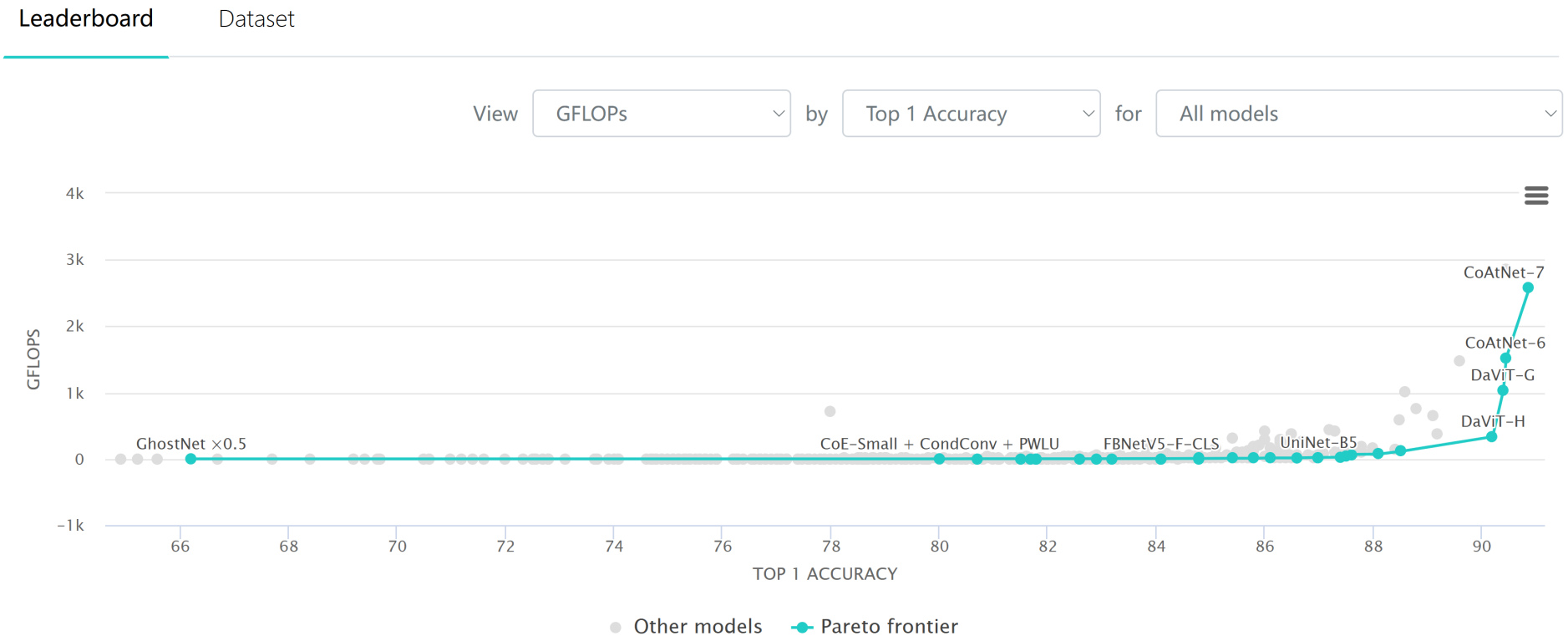



*Figure 7. The plot of the GFLOPs of model over Top 1 Accuracy (paperswithcode.com)*

# Image Classification on ImageNet

Leaderboard Dataset

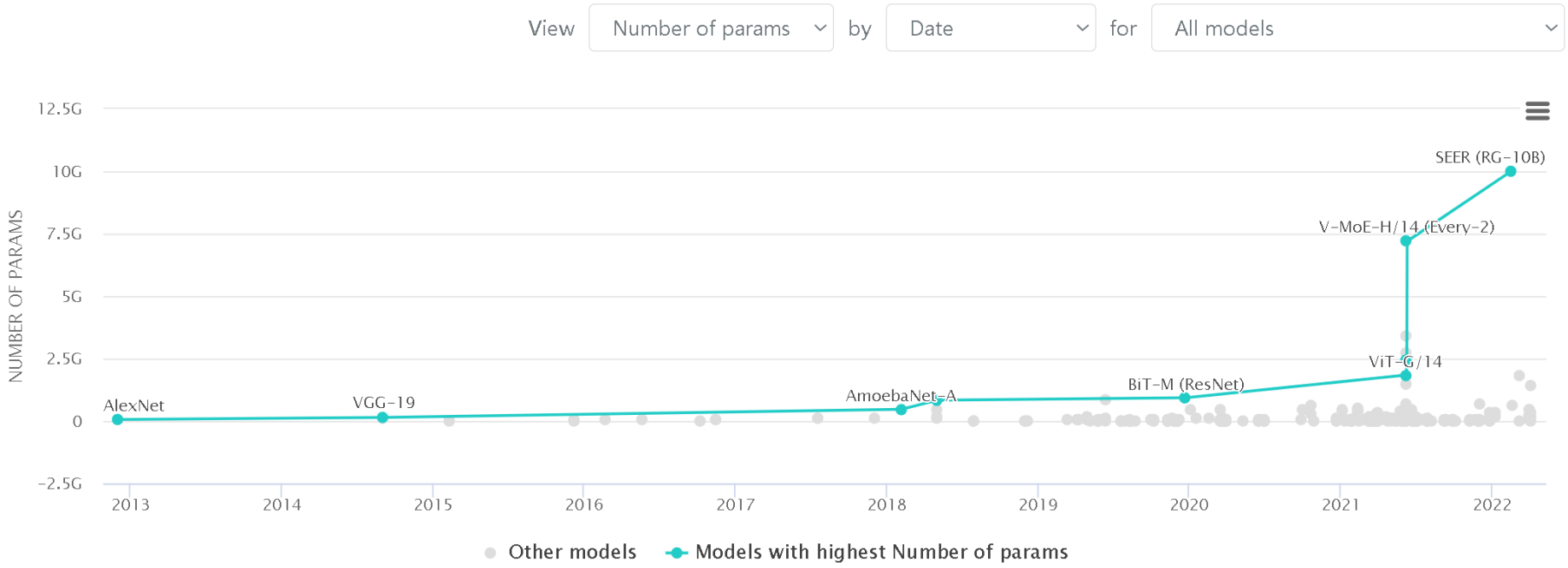



*Figure 8. The plot of the number of model parameters over time (paperswithcode.com)*

### 2.3.2 Natural Language Processing: Penn Treebank

Specifically, a subset of the English Penn Treebank (PTB) corpus corresponding to Wall Street Journal (WSJ) articles is one of the best-known and most often used corpora for assessing sequence tagging models, and it is also one of the most widely used corpora in general (Marcinkiewicz, 1994). In order to complete the challenge, you must annotate each word with the help of its lexical markers.

The process of predicting the next word or character in a document is accomplished through the use of Penn Treebank language modeling. Language models trained with this approach may be used for a variety of natural language tasks, including text production, text categorization, and question and answer tasks. Cross entropy and confusion are used to assess the models' ability to model language in various contexts. SuperGLUE (A. Wang et al., 2019) is one of the most recent and widely used benchmarks for testing language modeling skills.

In this area, pre-trained models show more absolute dominance in Test perplexity, but the model size is also absolutely gigantic. For those models that did not use extra data, their parametric numbers were basically around 22 million (Melis, Kočiský, & Blunsom, 2019; Dilin Wang, Gong, & Liu, 2019), and the difference between models was not very large, as shown in Figure 9. However, for models that use additional data, such as BERT-Large-CAS (C. Wang, Li, & Smola, 2019) and GPT models (Radford et al., 2019), the number of parameters is extremely large, especially GPT-3 (Brown et al., 2020). GPT-3 is most surprising in terms of model size, with a staggering 175,000 million parameters, and the largest dataset used is 45 TB before processing. According to OpenAI's arithmetic statistics unit petaflops/s-days (petaflops = flops*$10^{15}$), it takes about 1900 pfs-day to train AlphaGoZero, while OpenAI's proposed GPT-3 uses 3640 pfs-day. With the arrival of GPT4, everything is even more crazy. It has been estimated by scholars that the size of GPT-4 is 10 times more than GPT-3, with 1.8 trillion parameters. OpenAI used about 2.15*$10^{25}$ FLOPS in the training of GPT-4. In this area, the big companies have an absolute computing power advantage and their own private databases, and can easily win in an overwhelming manner in various metrics. The good news is that the products developed by the big companies now provide API for use by academics and industry worldwide.

# Language Modelling on Penn Treebank (Word Level)

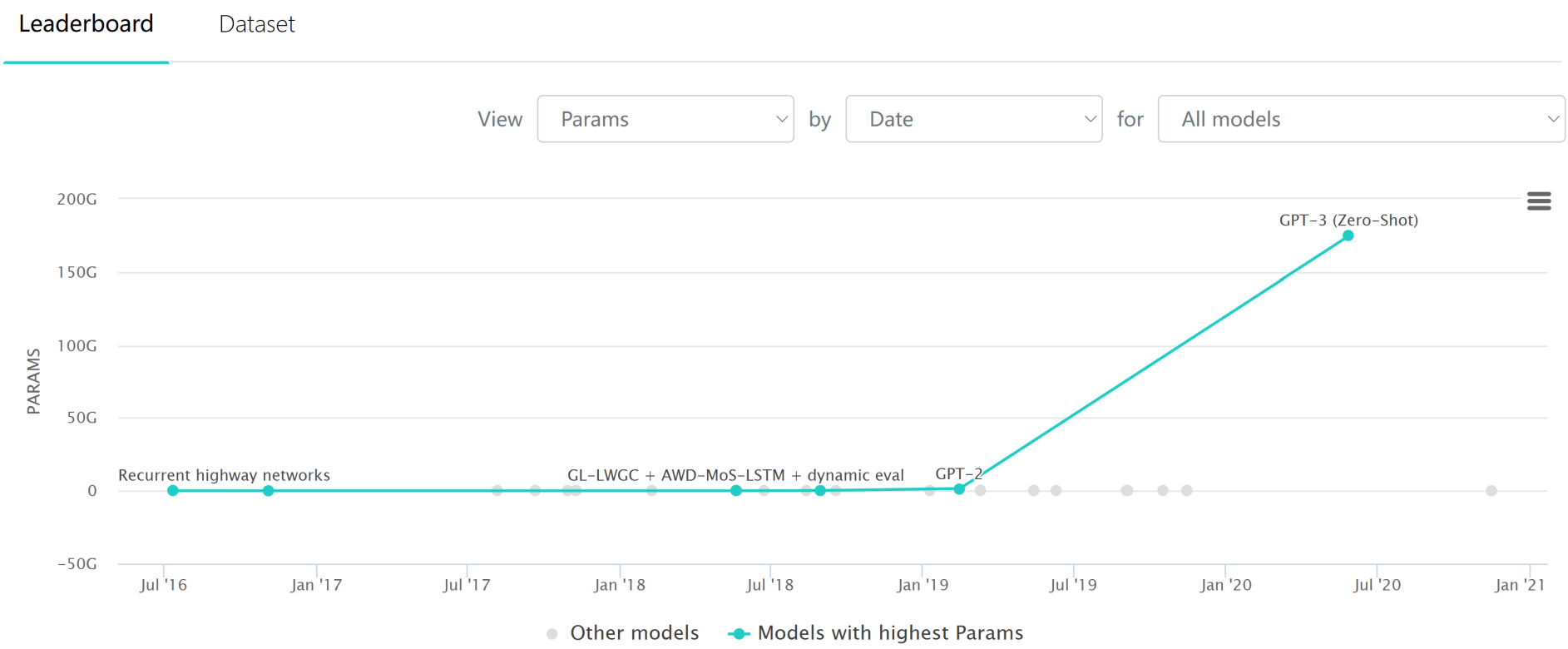



*Figure 9. The plot of the number of model parameters over time (paperswithcode.com)*

### 2.3.3 Structured Data: MIMIC-III

Both of these areas are of wide interest for unstructured data, as there is more information to be mined from this kind of richly implied data. However, structured data has been studied for a longer period of time and is now slowly fading out of sight. The classic examples of structured data are medical-related or financial-related data, which have been accumulated over the years in the form of tables. The following is an example of medical data.

In the Medical Information Mark for Intensive Care III (MIMIC-III) dataset (Johnson et al., 2016), information about patients admitted to large tertiary care hospitals' intensive care units is de-identified and made publicly available. The MIMIC-III dataset contains information about patients admitted to large tertiary care hospitals' intensive care units. Vital signs, medicines, laboratory measures, observations, and notes were taken by care providers, fluid balances, procedure codes, diagnostic codes, imaging reports, length of stay, and survival statistics are just a few of the types of information that can be collected. There are ICD-9 (Quan et al., 2005) codes associated with each entry in the dataset, which indicate the diagnosis and the procedure that was performed. Each code is further subdivided into sub-codes, which typically provide context-specific information about the code. Examples of applications that can be enabled by the database include academic and industrial research, quality improvement initiatives, and courses in higher education. In today's healthcare system, every healthcare delivery organization must be able to predict medical codes from clinical notes since it is a practical and essential requirement.

In this relatively more specialized and less popular field, the most obvious difference is less attention. Less attention means fewer papers and fewer models, and also results in less significant improvements in accuracy over the years as shown in Figure 10. This also reveals a limitation of the current development of the machine learning field, where resources are devoted to the popular areas, and scholars expect to chase high on the more popular rankings, while the unexplored areas are less sought after.

# Medical Code Prediction on MIMIC-III

Leaderboard Dataset

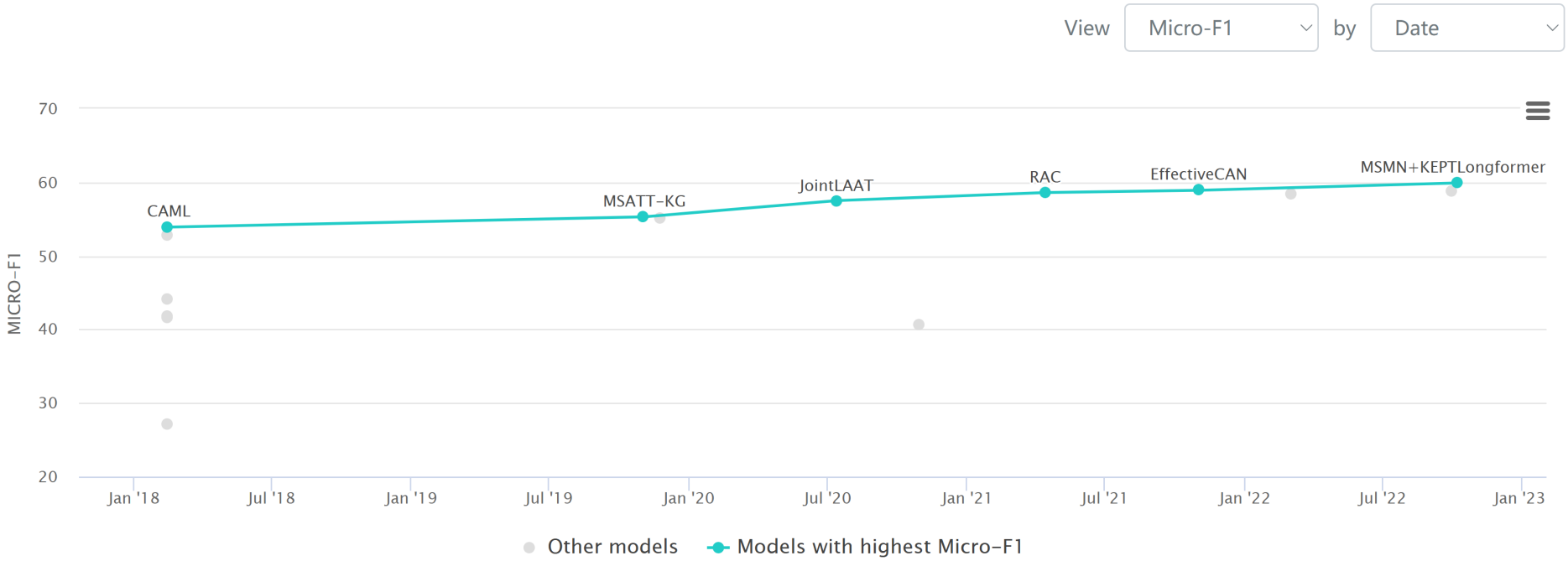



*Figure 10. The micro-F1 rate on medical code prediction problems (paperswithcode.com)*

*After analyzing the famous datasets as well as model development trends in the three fields, it can be found that the popular fields have fully enjoyed the development dividend of computing power development as well as a large amount of data, but the development has also slowly fallen into the dead-end of super-scale. Now, most traditional industries have collected a certain amount of business data, but the number is still small compared to these millions of machine learning datasets after all. Can these mega-complex models also show perfect performance on smaller datasets? This will need to be discussed further in a later section.*

And since cold fields have received less attention and there is still a big gap between the current state of development and the popular fields, how should these cold fields leverage the results of popular fields to develop themselves better? These questions will be discussed systematically in the next section.

## 2.4 The Compression and Customization of Machine Learning

Since the entire application process of machine learning models can be regarded as the fitting of machine learning algorithms on different data, some methods of compression and customization of machine learning have been adopted to help apply the algorithm more appropriately in specific application scenarios. This section will review the development of several algorithms and data fields related to compression and customization, including their origins, breakthroughs, and recent research. Then, some of the integrated studies are summarized to gain some insight into the research field .

Using neural networks to reduce the dimensionality of data, Geoffrey Hinton and his student Salakhutdinov published a paper in the journal Science titled “Reducing the Dimensionality of Data with Neural Networks(G. E. Hinton & Salakhutdinov, 2006(Geoffrey E Hinton & Salakhutdinov, 2006)” in 2006. A solution to the problem of gradient disappearance in deep network training is proposed in this article. It involves unsupervised pretraining to initialize weights, followed by supervised training to fine-tune them. Deep learning became popular in academics and industry as a result of this.

Looking back today, the ideas and thoughts presented in this thesis may be a bit outdated, but there is no doubt that this thesis has brought deep learning back to

people's views and has been unstoppable ever since.

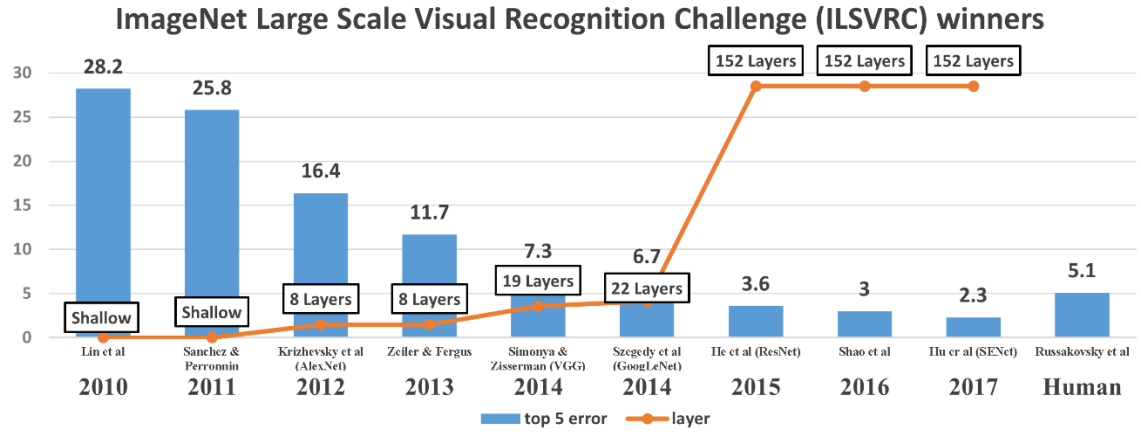



*Figure 11. Iterations of model accuracy and number of layers*

Since its return to the public eye, deep learning has been a lukewarm development and has not received a lot of attention from industries other than machine learning. The main reason for this is that for a long period of time, the accuracy of machine learning in application scenarios was low and consistently below human levels (5%-10% error rate). As shown in Figure 11 (Alom et al., 2018; Hu, Shen, & Sun, 2018; Y. Lin et al., 2010; Rawat & Wang, 2017; Russakovsky et al., 2015; Sánchez & Perronnin, 2011; Szegedy et al., 2015; Zeiler & Fergus, 2013), this all changed significantly in 2012, when Hinton's group, in order to prove the potential of deep learning, entered the ImageNet image recognition competition for the first time and won the championship by building the CNN network AlexNet, which crushed the classification performance of the second place (SVM method). In 2013, 2014, and 2015, through the ImageNet image GoogLeNet recognition competition, the network structure, training methods, and GPU hardware of deep learning continued to advance, leading to its conquest in other fields as well. The time reached 2015 when the world thought deep learning had reached its limit because of the gradient disappearance problem, ResNet came out, which greatly improved the number of layers of neural networks and achieved better results. After this, deep networks started to improve further with a larger number of parameters. It was not until 2017, when the last ImageNet image recognition competition came to an end and was no longer held, that people began to calm down and think about whether the price paid for achieving such extreme scores was worth it. So a more emerging field began to emerge, namely lightweight networks for edge computing. Lightweight networks hope to trade-off between accuracy and speed and

bring the power of machine learning to light in more industries.

Edge computing (J. Chen & Ran, 2019; Shi, Cao, Zhang, Li, & Xu, 2016) itself is also very promising, taking driverless cars as an example to briefly analyze the characteristics of real-time edge computing. Driverless cars require localized computing control centers' real-time reasoning and decision making when they are working. Because of the extremely short response time required for driving scenarios and the complexity of working scenarios with high privacy of data, it is difficult to transmit the data collected by the vehicle sensors to the cloud server to make judgments. Similar to driverless cars there are industrial robots, security cameras, augmented reality, and other applications that require real-time local computing at the terminal. Another feature of edge computing application scenarios is that the computing devices are more limited in computing power (limited by size and power consumption), so the deployment of the model puts forward more demanding requirements in the case of limited computing power. The evaluation of algorithms and models has also changed significantly, with the number of parameters, computation, memory access, training time, computation time, energy consumption, carbon emission, CUDA acceleration (Sanders & Kandrot, 2010), adversarial learning, and a series of other indicators being evaluated on the basis of accuracy.

Another important driving factor for edge computing to gradually come into everyone's view is that machine learning techniques are starting to be widely used in various industries to solve practical problems in some specific scenarios. When it comes to specific scenarios, users find that some of the functions and extreme accuracy in the original traditional large-scale models are not needed in normal working environments. In order to save resources, it is the rational demand of industry to use only the most needed functions in the large-scale model and with the most economical accuracy. In the use of the model, the applicability of the original model may also be slightly different from the actual working scenario, and the problem of model customization has gradually surfaced to the researchers in order to make the model perform better.

Based on the above-analyzed trends and realistic needs, this section reviews and discusses the existing methods for making models smaller and more specific to a fixed scenario.

### 2.4.1 The lightweight of Machine Learning

There are currently excellent solutions in academia and industry to meet the needs of mobile, terminal edge computing. There are three main types of software-level as well as one type of hardware-level solutions (S. Han, Mao, & Dally, 2015). They are: compression of already trained models, direct training of lightweight neural networks, accelerated convolutional operations, and hardware deployment. The main objectives are basically to reduce the number of model parameters, reduce the amount of model computation after deployment, reduce the time cost, etc. In the following review and analysis, the discussion will focus on the core ideas of these previous improvements and discuss quantitatively what kind of improvement can be achieved by these methods.

#### a) Compression of already trained models

**Knowledge Distillation**

Since Hinton introduced the concept of knowledge distillation in 2015, this technique has been widely used with model training in various scenarios (G. Hinton, Vinyals, & Dean, 2015). In industry, knowledge distillation is frequently employed due to the simplicity and efficacy of the "Teacher-Student Network Idea", which is a model compression approach and a training method based on the "Teacher-Student Network Idea (Gou, Yu, Maybank, & Tao, 2021)".The sophisticated and huge model is utilized as a Teacher, whilst the simpler Student model is used as a Student model. During training, the Teacher model is used to assist in transferring its knowledge to the Student model. The Student model, in contrast, has a relatively weak learning ability, so the Teacher model is used in order to improve the generalization ability and generalization ability of the Student model. This prediction exercise is carried out using the flexible and lightweight Student mini-model, rather than the sophisticated and cumbersome but effective Teacher model, which serves just as a mentor (G. Chen, Choi, Yu, Han, & Chandraker, 2017; Phuong & Lampert, 2019).

The most subtle concept of knowledge distillation is the Soft-target that is passed from the Teacher network to the Student network.

Hard-target: The original dataset is labeled with one-hot tags, except for the

positive tag, which is 1, and all the negative tags are 0. This output is equivalent to telling only the correct answer to the original image.

Soft-target: The output of the SoftMax layer of the Teacher model is the probability of the category, with each category assigned a probability, and the positive label has the highest probability. This output has both the correct answer and shows the similarity relationship between the individual answers.

The output of the SoftMax layer, in addition to positive examples, negative labels also carry a great deal of information about the inductive inference of the Teacher model. For example, if some negative labels correspond to much higher probabilities than other negative labels, it means that the Teacher model considers the sample to have some similarity with that negative label at the time of inference. In contrast, in the traditional training process (Hard-target), all negative labels are treated uniformly. That is, the training approach of knowledge distillation makes each sample bring more information to the Student model than the traditional training approach. It is this richer delivery method that allows the information analyzed and processed by the Teacher network to be delivered to the Student network in a more condensed manner. It also allows the student network to be slimmer (J. H. Cho & Hariharan, 2019; Yim, Joo, Bae, & Kim, 2017).

Another idea of knowledge distillation is the feature distillation method. It is not like the target approach described above, where the Student learns only the outcome knowledge like the Teacher's target, but learns the middle layer features in the structure of the Teacher's network. The earliest work using this model comes from the paper "FITNETS: Hints for Thin Deep Nets (Romero et al., 2014)", which forces the network responses of certain intermediate layers of the Student to approximate the network responses of the corresponding intermediate layers of Teacher. The response of the intermediate feature layer of the Teacher in this case is the knowledge that is passed to the Student, which is essentially the transfer of feature-level knowledge from the Teacher to the Student.

This transfer strategy can also be useful when discussing scenario-related problems. When the training data belong to a fixed scenario, their correlation with each other will be reflected in the Soft-target of the Teacher network, i.e., the ratio between positive and negative sample probabilities is relatively similar. The idea of knowledge

distillation can be used to extract the required scene information for the subsequent training and prediction.

The limitation of knowledge distillation is in the fact that the Student model can only go as far as the Teacher model can go, and not better. This greatly limits the realization of some specific needs.

**Pruning.** When used in actual applications, a big neural network contains considerable redundancy as a result of the limits of the particular application situation. It is possible to decrease this duplication through the use of pruning techniques (Reed, 1993). The underlying concept of pruning is to reduce the number of connections between neurons while guaranteeing that there is no significant loss of accuracy. It significantly decreases the amount of computation required and the number of weights required, while also increases the efficiency with which the network operates (LeCun, Denker, & Solla, 1989).

It was in decision trees that the pruning technique was originally applied, and it is an essential strategy for dealing with overfitting in decision trees (Mingers, 1989). In decision tree learning, the process of node partitioning will be done over and over again in order to categorize the training samples as accurately as possible. This will result in an excessive number of nodes in the tree. When this happens, it is possible that overfitting will occur because decision tree learning is so effective that it regards some attributes of the training set itself as qualities common to all data (Molchanov, Mallya, Tyree, Frosio, & Kautz, 2019).

Unstructured pruning removes unimportant neurons, and accordingly, the connections between the pruned neurons and other neurons are ignored in the computation. Since the pruned model is usually sparse and destroys the structure of the original model, this type of method is called unstructured pruning. The advantage of unstructured pruning is that it can greatly reduce the number of parameters and the theoretical computation of the model, and it is very simple to implement. However, the existing hardware architecture is not able to accelerate the computation, so it is not able to improve the actual operation speed and requires a specific hardware design to make the acceleration possible (Zhuang Liu, Sun, Zhou, Huang, & Darrell, 2018).

The opposite of unstructured pruning is structured pruning, which usually prunes

filters or entire network layers as the basic unit. When a filter is pruned, the previous feature map and the next feature map are changed accordingly, but the structure of the model is not destroyed and can still be accelerated by the GPU or other hardware, hence this type of method is called structured pruning (Z. Wang, Wohlwend, & Lei, 2019).

Compared with knowledge distillation, which "slims down" by enriching the information density, pruning is more like cutting off the fat in order to reduce weight. The idea of pruning is also more inspiring for scenario-based requirements. When the model is trained and some features in the scene are found to have little impact on the overall model, the network nodes related to these features can be pruned or structured to remove convolutional filters and kernel rows. Even the unimportant features can be identified before the training starts by the a priori knowledge the person concerned has to reduce the burden during training.

The limitation of pruning is also obvious; these trained nodes exist in some sense. If they are not needed at all, these nodes can be removed at the beginning of the model design. Once the model has been trained, removing these nodes with smaller weights will slim down the model but will also make it less accurate.

**Quantization of weight.** Model quantization is a technique for converting floating-point computation into the low-ratio specific-point computation (C. Zhu, Han, Mao, & Dally, 2016). Trained Ternary Quantization (TTQ) can effectively reduce model computation intensity, parameter size, and memory consumption, as well as speed up model inference. However, it often results in significant accuracy loss due to the reduction in the number of floating-point operations. For instance, when working with extremely few bits (4 bit), binary networks (1 bit), or even quantizing gradients, the accuracy difficulty is increased significantly. When compared to the higher precision kinds of FP32, the lower precision types of FP16, INT8, and INT4 take considerably less space, allowing for considerable reductions in both storage space and transfer time. Consider mobile phones as an example: in order to deliver more human and intelligent services, more and more operating systems and application programs (APPs) are incorporating deep learning, which necessitates the inclusion of a significant number of models and weight files. Take, for example, the conventional AlexNet model, whose initial weight file has grown to more than 200MB in size, and

the new models that have arisen in recent years, which are becoming more sophisticated in structure and include more parameters (Z. Cai, He, Sun, & Vasconcelos, 2017). It goes without saying that the spatial advantage of the lower precision kinds is still apparent. It is also more efficient to use low bits for processing, and the acceleration ratio of INT8 relative to FP32 may reach three times or even more, while the power consumption decreases as a result of this (S. Jung et al., 2019).

In general, quantization schemes are divided into two main types: On Quantization and Off Quantization, On Quantization refers to Aware Quantization and Off Quantization refers to Post Quantization. Perceptual training quantization is well understood according to the name, which is actually the quantization scheme used in the training phase of the network model. The quantization scheme in Post Quantization is not related to training, but is mainly used to quantize the model when it is an offline tool (model transformation tool) (D. Zhang, Yang, Ye, & Hua, 2018).

Weight quantization compresses the model by changing the storage format of the model, which is a new perspective like “abbreviation”. However, this also imposes more stringent requirements on the original format of the model, since only standardized models can be quantized in weights. This requires scholars in different fields to pay attention to the traditional machine learning model paradigm when exploring the applicability of machine learning in their own fields, in order to better serve their own fields with proven tools (e.g., weight quantization). Weight quantization can only be applied to data with values within a fixed range, once the values in the data are outside the range, weight quantization will not work properly.

All three approaches above compress the already trained models from different perspectives. The main purpose of knowledge distillation is to obtain a more streamlined model deployed on the endpoints, which improves the prediction efficiency. Pruning is the most effective means to compress the number of parameters, which can reduce the number of parameters significantly. Weight quantization can effectively record a large model in a more streamlined form, reducing the memory required for the model. Each of these methods has its own advantages and disadvantages and should be used on an as-needed basis, taking into account the final situation of the usage scenario.

### b) Direct training of lightweight neural networks

In different fields of machine learning, there are different techniques for model building, and how to design the network structure in such a way that the model has a smaller number of parameters and faster operation speed has been the goal of researchers. In the following section, three kinds of lightweight networks that are widely used in the field of machine vision are analyzed, with a view to exploring the design of lightweight networks.

**MobileNet.** In April 2017, Google proposed MobileNetV1, a lightweight neural network focused on mobile devices. The core concept of MobileNetV1 is Depthwise separable convolution (A. G. Howard et al., 2017).

Depthwise convolution deals with in-plane information and Pointwise convolution deals with cross-channel information. MobileNetV1 is built by stacking multiple Depthwise separable convolutions, and the breakthrough idea of MobileNetV1 is to use the emerging convolutional kernel construction method to achieve similar data processing results as the traditional method of standard convolution (e.g., VGG networks).

However, in the process of using MobileNetV1, it was found that the convolution kernels in the Depthwise convolution part are more prone to training failure - many of the convolution kernels from the Depthwise convolution training are empty. The authors analyze that it is because doing ReLU (Glorot, Bordes, & Bengio, 2011) operations in low dimensions can easily cause information loss. If the ReLU operation is performed in higher dimensions, the loss of information will be minimal. This also reminds future algorithm engineers not to use existing tools (e.g., activation function ReLU) as a matter of course when designing models, but to verify the applicability of the tools before using them carefully.

In order to overcome the problems of MobileNetV1, the Google team has made several improvements in MobileNetV2 (Sandler, Howard, Zhu, Zhmoginov, & Chen, 2018). Use inverted residuals: A shortcut structure is utilized in order to reuse features like ResNet. In addition, in order to overcome the information loss problem of ReLU in low dimensionality, the input data is first dimensioned up and then dimensioned down. For the low-dimensional data at the end of each module, the activation function

is switched from ReLU to Linear, which is a combination of separable convolution and residual connectivity to verify the synergy between the different methods. During the development of MobileNet from V1 to V3 (A. Howard et al., 2019), two activation functions customized for edge computing scenarios were also innovatively used, ReLU6 and h-swish, both of which can be more robust under low precision (float16) computation. This is a very bold approximation substitution that can be made to achieve better results when combined with scene information to meet specific needs.

**ShuffleNet.** ShuffleNet, jointly brought by MEGVII and Tsinghua research group at ECCV2018, also uses group convolution similar to MobileNet (X. Zhang, Zhou, Lin, & Sun, 2018).

This technique groups distinct feature maps from the input layer and then uses different convolution kernels to convolve each group, hence reducing the computing effort required for convolving each group. One issue with employing a group convolution layer is that the feature maps of various groups must communicate with one another in order for the network to be separated into numerous distinct routes, which will impair the network's capacity to extract features from data. ShuffleNet does not use dense pointwise convolution to meet the goal of feature communication, instead of relying on other ideas such as channel shuffle operation to compensate for information sharing between groups to achieve the goal of feature communication In other words, following group convolution, the feature map is "reorganized" so that the next group convolution is adopted with inputs from various groups, allowing information to flow across different groups of people and organizations. According to the authors of the ShuffleNetV2 study (N. Ma, Zhang, Zheng, & Sun, 2018), FLOPs are not truly comparable to speed as a metric of computational complexity, and networks with similar FLOPs might have very different speeds. The use of FLOPs as a measure of computational complexity is insufficient, as memory access usage and GPU parallelism must also be taken into consideration.

It is possible to deduce from the ShuffleNet concept that there are numerous potential solutions to a certain detailed problem (cross-group information flow). Compared to ShuffleNet, MobileNet uses more convolution, which is a disadvantage in terms of computation time and the number of parameters, but increases the number of nonlinear layers, which makes the features more abstract and advanced in theory;

ShuffleNet eliminates point-wise convolution and instead employs channel shuffle, which is simple and straightforward, eliminates the convolution step, and reduces the number of parameters; MobileNet employs point-wise convolution and instead employs channel shuffle, which is simple and straightforward when confronted with real-world use circumstances, a more appropriate algorithm should be selected based on the individual case.

**SqueezeNet.** SqueezeNet was published in ICLR-2017 by researchers from Berkeley and Stanford (Iandola et al., 2016), and the novelty of this research is the squeeze. A squeeze layer is proposed in this research, which uses a 1*1 convolution kernel to convolve the previous feature map. The main purpose is to reduce the dimensionality of the feature map and the number of input channels. By deferring the subsampled operation, a larger activation map can be provided to the convolutional layer: a larger activation map retains more information and can provide a higher classification accuracy. The network structure design idea, again similar to that of VGG, is stacked using convolutional operations.

The three most famous and widely used lightweight networks (MobileNet, ShuffleNet, SqueezeNet) in the field of computer vision, if viewed in outline, are simplified from traditional large-scale models such as AlexNet, VGG, GoogLeNet, and ResNet. Although each of them can be used to obtain a lighter model to some extent, they do not go beyond the original framework to design a new model paradigm. It is not possible to meet the richer and more precise demands of a complex model.

### c) Accelerated convolutional operations

As analyzed in Jia's paper (Y. Jia, 2014), convolution calculations take up the most time and consume the most resources in the model training process. Therefore, in the field of computational acceleration, the acceleration tools related to convolution calculations are the most abundant.

**Im2col + GEMM.** Im2col converts the different channels of a picture into columns of a matrix, that is, it converts the input 3D data into a 2D matrix. Through the conversion, the work of scanning the convolution kernel, which needs to be done several times, can be transformed into the work of multiplying matrices of larger size

at one time, so that the convolution calculation can be expressed as the multiplication of two 2D matrices. The computer reads similar memory at once is the fastest, especially when the data needs to be sent to the GPU for computation, so this saves the time of accessing memory for acceleration purposes. (Chellapilla, Puri, & Simard, 2006; Chetlur et al., 2014; M. Cho & Brand, 2017; Y. Jia, 2014) And Im2col with GEMM can provide better results. General Matrix Multiplication (GEMM) is one of the core computational units of the deep learning framework and is widely used in the implementation of operators such as Convolution, Full connection, etc. It is a library of tools for matrix computation acceleration, mainly by cutting, rearranging, and multi-threaded division of matrices. (M. Cho & Brand, 2017)

The strong combination of Im2col and GEMM shows that the discussion of the limitation problem can draw on the solution of the related problem and solve the problem in the original domain with the help of better tools. Of course, this approach has some limitations, when stride (stride is the number of lattice shifts per convolutional kernel step) < kernel size, a large number of duplicate pixels will be included in the transformed matrix, which is a challenge for memory usage.

**WinoGrad.** Nowadays, the mainstream mobile deep learning inference frameworks basically use the WinoGrad algorithm to accelerate convolution. The WinoGrad algorithm was first proposed by Shmuel Winograd in 1980 (Cooley & Winograd, 1980; Winograd, 1980) and did not create much of a stir at that time. At the CVPR 2016 conference, Lavin et al. presented "Fast Algorithms for Convolutional Neural Networks (Lavin & Gray, 2016)", which uses WinoGrad to accelerate convolutional operations. For the WinoGrad algorithm, it is essentially to lessen the computation by reducing the multiplication in the convolution operation. This is made possible by the fact that the matrix converted into the input signal in the convolution operation is not an arbitrary matrix with a large number of repeated elements distributed regularly (Yan, Wang, & Chu, 2020).

**Low-rank decomposition.** The rank of a matrix is a measure of the correlation between the ranks of the matrix. When the rank of a matrix is significantly smaller than the number of ranks of the matrix, such a matrix is called a low-rank matrix. Decomposition of a low-rank matrix removes redundancy and reduces the weight parameter (Bach & Jordan, 2005; S. Lin, Ji, Chen, Tao, & Luo, 2018). Since the weight

vectors are mainly distributed in some low-rank subspaces, the weight matrix can be reconstructed with a few bases (W. Wen et al., 2017).

It can be seen that in the field of accelerated computing, the complex operations in machine learning are basically simplified or transformed into a more computable form by computers through some mathematical techniques. In each specific academic field, there are mathematical formulas that have been proven to be feasible and effective. These formulas can be used as important knowledge points for machine learning in that field, and the formulas can be used as the leading ideas for designing machine learning models. This is not a bad way to develop the idea of scenario-based machine learning.

### d) Hardware deployment.

Hardware deployment is some of the ways to accelerate targeted functionality from the hardware side.

**TensorRT.** TensorRT is a C++ library that makes it possible to do high-performance inference on NVIDIA graphics processor units (GPUs) (Vanholder, 2016). When used in conjunction with training frameworks like as TensorFlow (Abadi et al., 2016), Caffe (Y. Jia et al., 2014), PyTorch (Paszke et al., 2019), and MXNet (T. Chen et al., 2015), it is specially intended to provide rapid and efficient network inference on graphics processing units (GPUs). TensorRT is already integrated into certain current training frameworks (e.g., TensorFlow), allowing it to be used to speed inference in the context of the framework. The TensorRT package, which provides parsers for importing existing models from Caffe, ONNX (Bai, Lu, & Zhang, 2019), or TensorFlow as well as for generating models programmatically (C++ or Python API), can be used in user applications as an alternative. After training a neural network, TensorRT may compress, optimize, and deploy the network during runtime, all without the need for a framework or other intermediary. When used in conjunction with other layering techniques such as kernel optimization selection, normalization and conversion to optimum matrix math methods depending on specified accuracy, TensorRT reduces latency, increases throughput, and increases network efficiency.

**OpenVINO.** OpenVINO is a comprehensive tool suite from Intel for the rapid

deployment of applications and solutions, supporting more than 200 CNN network structures for computer vision (Gorbachev et al., 2019). OpenVINO is a Pipeline toolset that is compatible with trained models from various open-source frameworks and has various capabilities for the online deployment of algorithmic models. With OpenVINO, you can easily deploy pre-trained models on Intel CPUs quickly. For AI workloads, OpenVINO provides Deep Learning Inference Suite, which can deploy trained models from various open-source frameworks online. In addition, it also includes OpenCV, an image processing toolkit, and Media SDK, a video processing toolkit, for image and video decoding, pre-processing, and post-processing of inference results.

**FPGAs Integrated Circuits.** Field programmable gate arrays (FPGAs) are integrated circuits with a programmable hardware architecture. The circuitry contained within the FPGA is designed to conduct a wide range of diverse purposes and may be reprogrammed to execute these activities as required by the user. After they have been created, FPGAs may be configured by the user for specific applications. FPGAs are comprised of Adaptive Logic Modules (ALMs) and Logic Elements (LEs), which are coupled by programmable interconnects to form a digital circuit (Monmasson et al., 2011; Rodriguez-Andina, Moure, & Valdes, 2007). When assembled together, these blocks form physical arrays of logic gates that may be tailored to execute certain computer tasks. The disadvantages of ASIC chips are also apparent. Because ASIC chips are designed for specific applications, the chip can handle a single algorithm, when the algorithm changes, the ASIC chip designed for the previous algorithm can not be updated accordingly. Especially in such areas as AI, in the case of various algorithms continue to iterate, the fastest speed to commercialize cutting-edge technology is also one of the important criteria to be considered.

In terms of hardware deployment, hardware and software companies are making efforts to deploy as many newer and faster models as possible for commercial use. This also means that the widespread use of machine learning in various fields is about to become a reality, which puts a demand on customized machine learning. This is because it is not possible to have the current general-purpose machine learning models to solve all segments of problems in all domains. Next, the development of custom machine learning will be examined.

### 2.4.2 Customization of Machine Learning

Since the development in the field of machine learning in recent years is still mainly in the direction of how to be faster and more accurate, the work of how to apply it in specific industries is mainly done by industrial companies, so the exploration of custom models is more limited. This subsection will focus on the currently widely used means of applying generic models to specific applications.

#### a) Transfer Learning

Exactly as its name indicates, transfer learning is the practice of transferring previously learned model parameters to a new model in order to aid in its training. The fact that most data or tasks are correlated allows us to share the learned model parameters (which can be interpreted as the knowledge learned by the model) with a new model in some way in order to speed up and optimize the learning efficiency of the model without having to start from scratch as is the case with most networks today (C. Tan et al., 2018b; Torrey & Shavlik, 2010; Karl Weiss, Taghi M. Khoshgoftaar, & DingDing Wang, 2016; Zhuang et al., 2020).

Since AlexNet started the research trend of deep learning in 2012, deep transfer learning has evolved from the simplest and most effective Pre-train and Fine-tune to today's burgeoning Domain Adaptation (DA), to the recent explosion of Domain Generalization (DG). While witnessing numerous researchers' efforts, transfer learning has also undergone remarkable development.

**Fine-tuning.** Fine-tuning is a way to modify the original trained model to fit a new dataset. Some nodes of the model are retrained or continue to be trained according to the new data (Tajbakhsh et al., 2016). This simplest and most commonly used method also has its limitation, as it performs poorly when the amount of data is small or when the new dataset differs significantly from the original model training dataset.

**Domain Adaptive.** To do this, data from distinct distributions in the source and target domains are combined and mapped into a feature space. The goal is to identify a metric in the feature space that brings the feature distributions of data from the source and target domains closer together as feasible. To increase accuracy on the target domain, it is possible to migrate the objective function trained on the source domain

in the feature space, i.e., the discriminator trained on the features of source domain data, over from the source domain (Cortes & Mohri, 2014; Ghifary, Kleijn, & Zhang, 2014).

(1) Sample adaptation: The basic idea is to resample the source domain samples so that the distribution of the resampled source domain samples and the target domain samples is basically the same, and to relearn the classifier on the resampled set of samples (Das & Lee, 2018).

(2) Feature-layer adaptation, which projects the source and destination domains into a common feature subspace. The basic idea is to learn a common feature representation, where the source and destination domains are distributed as identically as possible. Through feature adaptation, the incoming samples are projected into the common subspace, and the empirical errors in the source domain are calculated to approximate the distribution of the empirical errors in the target domain to be the same (M. Long, Wang, Ding, Sun, & Yu, 2013; L. Song et al., 2020).

(3) Model-level adaptation: The error function of the source domain is modified to consider the error of the destination domain. There are two approaches to model adaptation: one is to model the model directly, but add the "proximity between domains" constraint to the model, and the other is to use an iterative approach to progressively classify the samples in the target domain, add the samples with high confidence to the training set, and update the model (Ngiam et al., 2018).

**Domain Generalization.** In recent years, Domain Generalization (DG) has been an extremely prominent study direction (Da Li, Yang, Song, & Hospedales, 2017; K. Zhou, Liu, Qiao, Xiang, & Change Loy, 2021). A generalization-competent model must be learned from numerous datasets (domains) with varied data distributions in order to produce superior results on an unseen test set, and this research studies how to accomplish this goal. While there are some similarities between the Domain Generalization problem and the Domain Adaptation (DA) problem, the most significant difference is that in the DA problem, both source and target domain data are available for training while in the DG problem, only a limited number of source domain data are available for training and no test data are available. There is little doubt that DG is a more difficult and practical scenario to deal with than the DA scenario (Jindong Wang et al., 2021).

The existing domain generalization methods can be divided into three major aspects: data manipulation, representation learning, and learning strategies.

(1) Data manipulation refers to the enhancement of training data by augmenting and changing the data. This category includes two major parts: data augmentation and data generation.

(2) Representation learning refers to the learning of domain-invariant representation learning to make the model adaptable to different domains.

(3) Learning strategy refers to the introduction of proven learning patterns from machine learning into multi-domain training to make the model more generalizable.

It goes without saying that transfer learning is one of the most challenging topics in machine learning. Understanding transfer learning not only enables us to better comprehend the learned characteristics but also provides us with a new perspective on the nature of neural networks and how they "learn". The connection of various tasks is assumed by everyone when conducting transfer learning, however how to define correlation and how to statistically represent the level of correlation between tasks is a subjective judgment that favors humans when doing transfer learning. ImageNet is frequently utilized as a pre-trained model for fine-tuning since the big dataset of ImageNet itself assures that the learned network has a high degree of generalization. However, what happens when a small dataset is used? Is the outcome going to be the same? Or will it be worse than a network that has been built from the ground up?

DeepMind's new AlphaGo Zero was created entirely from scratch and is far superior to the previous version, AlphaGo, which was based on human graphs and hence less accurate. All of this is something that should be taken into consideration while implementing transfer learning.

### b) Data augmentation

Transfer learning systems that highlight the notion of data augmentation appear to be quite popular, according to a survey analysis of the field. It is the purpose of this part to gain an understanding of the application of data augmentation in customization studies (T. Nguyen & Pernkopf, 2019; Tanner & Wong, 1987; Van Dyk & Meng, 2001).

Expanding the value of limited data by making it provide value comparable to greater data without considerably increasing the data is referred to as data augmentation or data expansion. Data augmentation refers to data augmentation based on existing data that is carried out in accordance with predetermined data transformation rules. Generally speaking, when single-sample data augmentation is used (i.e., when only a sample is augmented), all operations are done around the sample itself (including geometric transformation classes, color transformation classes, and so forth). Multi-sample data augmentation methods, as opposed to single-sample data augmentation methods, make use of numerous samples to produce new samples. There are a number of widely used approaches.

**SMOTE.** SMOTE is a interpolation-based method that can synthesize new samples for small sample classes to deal with sample imbalance and thus improve classifier performance (Chawla, Bowyer, Hall, & Kegelmeyer, 2002).

**SamplePairing.** The SamplePairing method is based on this principle (Inoue, 2018). Simple data enhancement operations (such as random flipping, etc.) are performed on two randomly selected images from the training set, and then the resulting pixel averages are superimposed to create a new sample that is labeled with one of the original samples' labels.

**Mixup.** Mixup is a data augmentation method based on the neighborhood risk minimization principle proposed by the Facebook AI Institute and the Massachusetts Institute of Technology in "Beyond Empirical Risk Minimization (H. Zhang, Cisse, Dauphin, & Lopez-Paz, 2017)" which uses linear interpolation to obtain new sample data from the original data.

SMOTE, SamplePairing, and mixup share the same idea of trying to fit the true sample distribution by continuous increasing the discrete sample points, but the added sample points still lie within the region bounded by known small sample points in the feature space. A better data augmentation might be achieved if proper interpolation could be done outside the given range. Or adding a distinct tendency to the data augmentation would bring a different result. In other words, these methods can only create "something out of something" but not "something out of nothing". This has led to a lack of clear direction in these enhanced approaches, which can only be extended in general terms. They are still tools that serve a general-purpose algorithm.

### c) NasNet

NasNet is a Google architecture for large-scale image classification and recognition, that is distinguished by two layers designed by AutoML: the Normal Layer and Reduction Layer (Zoph & Le, 2016). The NasNet architecture is also distinguished by the fact that it does not require relevant experts to use human knowledge in the construction of the convolutional network architecture, which is a significant advantage. As a result, it is no longer essential for professionals to employ human knowledge to construct convolutional network architecture, and the Hyperparameter is computed directly by RNN, allowing for the realization of AI automated learning. The mobile MNasNet (M. Tan et al., 2019) is based on the NasNet, which transforms the design problem into a multi-objective optimization problem, using a reinforcement learning to search a deep convolutional neural network, but there are two main optimization goals, considering both accuracy and actual inference time consumption. Most previous search methods search for the optimal unit first and then stack them into a network, which can optimize the search space but suppress layer diversity. To solve this problem, the NasNet proposes a decomposed hierarchical search space (factorized hierarchical search space), which allows layers to have structural differences while still balancing flexibility and search space size well. From the results, the multi-objective optimization is a good balance between low consumption and accuracy, and the proposed search space can simultaneously reduce the time consumption and improve the accuracy.

This is a model-building approach that is completely customized to the dataset. During the training process, the model autonomously chooses: the convolution method (regular convolution, depth-separable convolution, inverse residual convolution), the convolution kernel size, and other parameters. However, the cost of searching for an optimal solution is very high. On 64 TPUv2 devices ($6.7 per hour), each model search process takes 4.5 days to complete. And during training, each model was run through the single-threaded large CPU core of the Pixel 1 phone to measure the true latency of each sampled model. In total, about 8K models were sampled. It is arguably very expensive, and for a dataset of countless various domains, such a large cost is rarely affordable.

## 2.5 Limitations of Current Machine Learning Models

As previously shown, the differences between data and compatibility issues were ignored. This neglect leads to the difficulty for complex models for complete scenarios to perform consistently on all problems (C. J. Cai et al., 2019; Harrison, Hanson, Jacinto, Ramirez, & Ur, 2020). There will always be particular problems that are substantially off in prediction, and there will always be images that cannot be correctly classified. Aim not only for the overall average performance of the model, but also to ensure that the worst performance of each problem is acceptable.

In the field of problem-based machine learning research, there has been minimal exploration of this. Christopher M. Bishop proposed a model-based machine learning by adopting a Bayesian viewpoint (Bishop, 2013), coupled with probabilistic graphical models and deterministic approximate inference algorithms to create a custom model tailored specifically to each new application.

However, these solution ideas are still rarely discussed for very specific individual problems, and this thesis will try to fill the gap and demonstrate the feasibility.

## 2.6 Summary

It can be seen that various research points or innovations can be found in machine learning models and data analysis since these two tools originated. Meanwhile, their great success has been accomplished in the application of real-life projects. Lately, other useful tools or theories, such as the hardware acceleration theory, have been incorporated, which has brought new research or application opportunities. The integration studies of machine learning models and data analysis under specific scenes are relatively inadequate, especially in recent years. Academic researchers tend to focus on general-purpose full-scenario machine learning algorithms to solve any problem.

For a summary of the research gaps: 1. The obsession with models with a huge number of parameters and a particularly wide range of applicability formed during the development of the field of machine learning has led to a bottleneck in the direction of development. 2. Machine learning models at this stage cannot take full advantage of

the rapid progress in computational computing and the high rate of data accumulation. 3. The current transfer learning approach and lightweight models cannot meet the needs of the industrial and medical fields in terms of the accuracy of models for specific problems, the need for scenario customization, and the need for lightweight devices.

Based on these research gaps, the problem statement and the research objectives in the INTRODUCTION chapter were summarized. Standing on the shoulders of giants, we can see farther. With the guidance of our predecessors, the future research path will be clearer.

*Transition Paragraph: Transitioning from the literature review detailed in Chapter Two, which underscores the evolution of machine learning algorithms and their foundational concepts, Chapter Three introduces the methodology employed in this thesis. It builds upon the need for customization and specialization in machine learning, as identified through historical and current advancements. Chapter Three methodically outlines a positivist and quantitative research framework to explore how changes in ML algorithms impact computational speed and accuracy. This approach not only contextualizes the theoretical aspects discussed previously but also paves the way for practical applications and ethical considerations integral to developing tailored machine learning solutions.*

# CHAPTER 3 METHODOLOGY

This chapter present the adopted methodology in the thesis, which is divided into the following three parts: Overall research approach from the theoretical level, research design for different parts, and discussion about ethics-related issues.

## 3.1 Overall Research Approach

**Introduction to Research Methodologies.** In academic research, the choice of methodology is pivotal as it shapes the entire framework of the study, guiding the researcher in data collection, analysis, and interpretation. Research methodologies are generally categorized into three primary approaches: positivism, interpretivism, and post-positivism (Archer, 1995; Bryman, 2016; Shapere, 1964).

Positivism. Positivism is a research philosophy commonly employed in the natural sciences, including fields like business and economics. It relies on observable and measurable facts, advocating for the use of quantitative methods to test hypotheses and validate theories. Positivism is grounded in the belief that reality is objective and can be understood through empirical evidence. This approach emphasizes detachment and objectivity, aiming to produce results that are generalizable and replicable.

Interpretivism. In contrast, interpretivism is often used in the humanities and social sciences. It focuses on understanding the subjective meaning of human experiences and social phenomena. Interpretivist research employs qualitative methods, such as interviews and observations, to explore the depth and complexity of social interactions and cultural contexts. This approach acknowledges that reality is constructed through human perceptions and interactions, making it inherently subjective.

Post-Positivism. Post-positivism bridges the gap between positivism and interpretivism, acknowledging the complexity of reality. It recognizes that while an objective world exists, our understanding of it is inherently influenced by our subjective experiences. Post-positivist research often combines both quantitative and

qualitative methods, aiming for a more nuanced understanding of phenomena.

**Justification for Choosing Positivism.** The main philosophy of research adopted is from Positivism (Ayer, 1959; Y. S. Park, Konge, & Artino, 2020). This study mainly explores the impact of changes in machine learning algorithms on the results of accuracy and computing speed. It is necessary to compare the advantages and disadvantages of various methods using facts and rigorous data analysis to test conclusions or hypotheses. The general approach is through data analysis, and then the candidate determines whether there is a correlation or causal relationship between the phenomena. If there is a certain connection between phenomena, hypotheses are established, and models are constructed to explain the relationship between phenomena. Positivism emphasizes observable phenomena and empirical data, which perfectly aligns with the goals and nature of this study (Patton, 2014; Popper, 2005). This is because the research primarily relies on quantifiable data and rigorous experimentation to test its hypothesis—that custom model based on specific scenarios benefits the models' performance in particular applications more than general-purpose model.

The empirical nature of this work, which includes validating models using real-world datasets (e.g., Hepatitis C dataset, UCI heart disease dataset), underscores the necessity of positivist methodologies. Furthermore, the research employs the scientific method, a logical reasoning process that systematically investigates proposed hypotheses. This method involves formulating hypotheses based on existing literature, designing experiments, collecting data, and analyzing results to draw conclusions. The structured and systematic nature of the scientific method is crucial for research dealing with complex machine learning algorithms and their performance across various scenarios. By adhering to positivist methodologies, this research ensures that findings are based on measurable and observable phenomena, thus enhancing the reliability and validity of the results.

Objective Analysis and Quantitative Focus. One of the core tenets of positivism is objectivity. This research aims to objectively evaluate the performance of scenario-

based machine learning models compared to general-purpose models (Denzin & Lincoln, 2011; Djamba, 2002). The use of standardized metrics and statistical analysis to compare model accuracy, efficiency, and adaptability supports the objective stance of positivism. This objectivity is crucial in making unbiased conclusions about the superiority of customized models in specific scenarios and provide clear guidance for the modification of approaches. Positivism emphasizes quantitative research methods, which are central to this study. The research involves the quantitative analysis of machine learning model performance, using metrics such as accuracy rates, computational speed, and efficiency. By adopting a positivist approach, the research can leverage statistical tools and techniques to analyze large datasets and draw meaningful conclusions about the effectiveness of scenario-based models. Different measurement standards come with certain limitations to the applicable scenarios, which should be avoided in the process of application.

Reproducibility and Generalizability. Positivism advocates for research that is reproducible and generalizable. The methodologies and models developed in this research are designed to be reproducible, allowing other researchers to validate and build upon the findings. Furthermore, while the models are customized for specific scenarios, the underlying principles and methodologies can be generalized and applied to other contexts, demonstrating the broader applicability of the research. This reproducibility ensures that the findings are not only reliable but also contribute to the wider body of knowledge in machine learning and artificial intelligence.

## 3.2 Research Design

The following research designs have been carried out under the guidance of Positivism and quantitative research. The discussion of algorithms and models within the domain of machine learning is inherently tied to three pivotal elements: data, models, and deployment. This trifecta aligns with the sequential phases of the workflow, which encompass data collection and processing, as well as the design and training of model architectures, followed by validation, optimization, and deployment.

Consequently, the ensuing discourse in this thesis predominantly adopts this tripartite division as its structural basis.

### 3.2.1 Scenario-Based Data Processing

In the whole process of machine learning, data is the most closely related to the scene. Data itself is the digital reflection form of the scene. Unfortunately, data is a "sincere" recorder of the real world. It does not speak and has no consciousness but can only save the information truthfully. This is different from the situation when humans face information in the external environment. Humans will selectively pay attention to the key points in the scene; for that unimportant environmental information, humans will scan indifferently to leave a general impression, not too much attention. However, humans also need these scenes because they have different tendencies to make judgments in different scenes.

Therefore, this thesis proposes to pay more attention to the more important information in the data set, while keeping the less important scene information. In other words, it is needed to understand the data with a deliberate "bias" to process the data and find the most relevant data to the problem. So how do you determine which information is important and which is less important? This requires both the scenario user and the data itself to determine the importance of the data.

**a) Scenario user's perspective.**

When a labeled item of the data contributes significantly to the result in a scenario, it means that this labeled item of the data is important and should be paid attention to. This kind of judgment is what scenario users are good at, and as someone, who has some experience working in the field, his understanding on the key signature variables is a must.

Likewise, for unimportant labeled items in the data, the scenario user will find the impact of this variable to be inconsequential in his or her daily work.

Scenario users can make a general judgment about the data when they get it, they

judge which variables are important and which are not. However, superficial human cognition is not enough to determine the causal relationship between variables in a short period of time, so if human beings are let intervene in the screening of data at the early stage of data processing, it will transfer the inaccuracy of human's own judgment to the data. Therefore, it is more sensible to let the users of the scenario review the trained model to check whether the important difference between the weights in the model is in line with the objective laws of the real world, so as to ensure the reliability and interpretability of the model.

**b) The perspective of data.**

The data itself will naturally present differences in the influence of different variables, and will also show the relationship between different data samples. The general process of machine learning mainly describes the relationship between variables, but not much attention is paid to the relationship between samples. The scenario-based data processing proposed in this study is going to fill this gap and explore how to use the relationship between samples to improve the accuracy of the model. The effect of focusing on some of the key samples can be achieved by modifying the ratio of the number between samples, just like a person focuses on the key information in a scene.

### 3.2.2 Scenario-Based Model design

The design of the machine learning model greatly affects the final result of calculation. A large and redundant model will lead to low efficiency, while an excessively lightweight model will not meet the accuracy requirements. If we start to think about the problem directly from the structure of the model, we will fall into the trap of idealism. Or one can only think like the previously mentioned idea of building lightweight models, where only certain functions can be replaced on the original traditional model to achieve the lightweight effect.

What this thesis proposes is to let the model only need to target a specific target

problem or a specific target problem set, and when a model becomes more singular in its functionality, it naturally becomes less bloated. The model only needs to be able to accomplish the simple problems it is given, and no longer needs to deal with a wide variety of problems. This idea fits well with real-world scenarios in various industries: most of the work is broken down into small tasks to be performed by different people: assembly line workers have a single and repetitive job; and hospitals are divided into different departments for diagnosis and treatment of specific diseases by specialized doctors. The single-task model can be replicated in countless areas as long as it performs the desired task with high quality. This single-task model has a single function and involves a small data size, so the model complexity and number of parameters are necessarily small. This can shorten the training time and train the newly collected data in real-time, while reducing the computing time after deployment and improving the efficiency of the end product.

### 3.2.3 Scenario-Based Validation and Optimization

Once a model has been built for a single problem, a question arises. How can the effectiveness of this new model be evaluated? In the past, all-purpose models were evaluated by reserving a separate portion of the collected data as the validation set and then tuning the model by evaluating the performance of the trained model on the validation set. Model validation in a scenario-based approach involves a meticulous process of ensuring that the model performs well on the intended task and is robust across various conditions within the scenario. Instead of relying solely on generic metrics (like accuracy, precision, and recall), validation should incorporate scenario-specific performance indicators that reflect real-world applicability and usefulness.

However, such a process is no longer applicable to small sample sizes. First of all, samples in a small sample space are already very rare, and each unique sample contributes significantly to the complexity of the entire sample space. Once some samples are stored separately as validation sets and do not participate in the training process, the training effect of the model itself will be greatly affected. If evaluated by K-Fold Cross-Validation (Y. Jung, 2018; T.-T. Wong & Yeh, 2019; Yadav & Shukla,

2016), it again suffers from the loss of accuracy when the final model is fitted. Special validation methods should be developed. For instance, if the model is designed for a healthcare application, its validation could include clinical relevance, diagnostic accuracy on specific conditions, and even user feedback from healthcare professionals. Scenario-specific metrics: Develop and employ validation metrics that are directly relevant to the scenario's outcomes, such as cost savings in an industrial setting or patient outcomes in healthcare.

Optimization in scenario-based machine learning should focus not just on improving model performance in a general sense but on ensuring that the model is optimized for the specific nuances and requirements of the scenario. For example, a feature-based selection and engineering approach in engineering informatics (Chandrashekar & Sahin, 2014; A. Sharma & Dey, 2012; Verdonck, Baesens, Óskarsdóttir, & vanden Broucke, 2021; A. Zheng & Casari, 2018) emphasizes the importance of representing phenomena through characteristic and parametric features. This approach prioritizes the model's key behaviors based on the relevance of engineering features to the scenario, naturally discarding generalist features that do not contribute to scenario-specific objectives. Another optimization method involves hyperparameter tuning, which should be conducted with the specific needs of the scenario in mind. This might involve prioritizing speed and efficiency over complexity if the scenario demands real-time performance, or the opposite if the scenario allows for more complexity. Additionally, it is crucial to closely examine cost-sensitive learning. In scenarios where certain types of errors are more consequential than others, implementing cost-sensitive learning can help minimize the most critical errors, ensuring that the model's performance aligns with the scenario's specific requirements.

## 3.3 Ethical Considerations

The data involved in this thesis are all data obtained from publicly available sources and have been properly cited according to the data publisher's requirements. Some of the data related to case information of some patients, where information

related to identity has been removed or desensitized by the data publisher so as not to reveal the privacy of the patient.

This series of studies may eventually be used in industry-specific work, so this study was conducted with as much detail as possible to document and analyze the various scenarios so that other researchers or industrial, medical professionals can use the methods in this study safely and efficiently.

## 3.4 Summary

This chapter introduces the general guiding principles for the entire study from a thoughtful scenario-based machine learning perspective. At its core, it delineates the strategic planning of the three quintessential segments of the research process, i.e. the collection and processing of data, the design of the model and the optimization of its parameters, and finally, the deployment. It offers a foundational analysis for each segment, coupled with a set of universally relevant approaches.

A concrete manifestation of the principles articulated in this chapter can be seen in Figure 3, which shows the integration of scenario-based machine learning models into an overarching framework.

*Transition Paragraph: Following the groundwork laid in the first three chapters, we have comprehensively discussed what scenario-based machine learning is, why it is necessary, and the gap between current real-world conditions and the ideal state we envision. The next three chapters will delve into the specific operations and innovative practices of scenario-based machine learning from various perspectives, demonstrating its superior performance.*

# CHAPTER 4 MACHINE LEARNING MODELS TAILORED TO A SINGLE INDIVIDUAL OBJECT

## 4.1 Introduction

This section will focus on the shortcomings of traditional machine learning that are primarily addressed in this chapter as well as some conceptual proto-rational analyzes of machine learning models tailored to single individual objects. Some of the definitions covered in this section are consistent throughout the thesis.

### 4.1.1 Problem Analysis

Applying machine learning to decision-making processes of significant consequence requires substantial courage, as decisions are directed not merely towards a set of cold data but also impact the life trajectories of involved individuals. This demands exceedingly high standards for the stable and superior performance of machine learning on individual objects. However, the current machine learning domain faces the following deficiencies, hindering the real-world application of machine learning models.

**The Demand for Improved Accuracy and Efficiency.** The accuracy and efficiency of machine learning models are crucial for success in specific application domains (F. C. A, K, & Christopher) (F. C. A, K, & Christopher) (C. L) (Omar, Paul, S, G, & K) (K. H. Park, Chung, & Kwon; Ravita & Deepinder). Yet, existing general models often fail to capture the subtle differences between individuals, which could decisively influence the predictive performance of the model (Fang, Annis, Elston-Lafata, & Cykert; Garcia-Ceja, Riegler, Kvernberg, & Torresen; R. V. Shah et al.; S. Taylor, Jaques, Nosakhare, Sano, & Picard). For instance, in the healthcare domain, individual differences in physiology, lifestyle, and environmental factors can significantly affect disease progression and treatment outcomes (Hopkins; Lopes-Ramos, Quackenbush, & DeMeo; Rockwood; Uher), factors often overlooked in traditional model training processes. The primary cause of this challenge is the diversity and complexity of data. Each individual is unique, and its feature data set encompasses a vast array of variables, which may vary significantly across

different individuals. Moreover, the non-stationarity of individual data increases the difficulty of model training, as the states and behavior patterns of individuals change over time. Traditional general models struggle to update in real time to keep up with such changes, potentially leading to decreased accuracy (Maccio, Chiang, & Down, 2014; Nasri, Kargahi, & Mohaqeqi; Uddin, Rizvi, Hashmani, Jameel, & Ansari, 2019; X. Wang, Qu, Wu, Wang, & Zhou).

**Addressing Data Imbalance Issues.** Data imbalance is a pervasive issue in machine learning, particularly in classification tasks (A'fifah, Ritahani, & Ahmad; Abokadr, Azman, Hamdan, & Amelina; Gautam & Dey; Pradeep Kumar, Bhatnagar, Gaur, & Bhatnagar; Rifqi & Deni; Thabtah, Hammoud, Kamalov, & Gonsalves). In many cases, samples of certain categories far outnumber others, causing models to bias towards predicting the majority class and neglecting the predictions of minority classes. This is particularly critical in domains such as medical diagnosis and financial fraud detection, where the number of positive samples (e.g., rare diseases, fraud cases) is much lower than negative ones. The fundamental cause of data imbalance lies in the inherently unbalanced distribution of real-world events (Byron, Kevin, C, & T; k. H, H, & A; S. J; Lincy & Seetha; T, R, & N). Additionally, biases in the data collection process can also lead to data imbalance. For example, hospital data mostly comes from individuals seeking medical care, making it easier to collect data on diseases with noticeable symptoms while data on specific groups, such as those with invisible or chronic illnesses, may be harder to obtain.

**Enhancing Model Interpretability and Transparency.** As machine learning models, especially deep learning models, become increasingly complex, their internal decision-making processes also become more difficult to understand. This "black box" characteristic makes the decision-making process of the models lack transparency, thereby reducing users' trust in the model outputs and causing limitations in application scenarios requiring high interpretability (Alexandra, Dongyu, R, & K; Bhatt, Ravikumar, & Moura; C; Rudin; Tiwari, Dubey, & Kumar; Yoon, Torrance, & Scheinerman). This is especially true in life-altering decisions, such as medical decisions, where uninterpretable models struggle to gain patients' trust. The complexity of the models is the main reason for issues with interpretability and transparency (Bell, Solano-Kamaiko, Nov, & Stoyanovich; Christoph,

Giuseppe, & B; Linardatos, Papastefanopoulos, & Kotsiantis; Molnar, Casalicchio, & Bischl, 2020; W, G, Alexander, Sebastian, & K). In attempts to capture the complex relationships in data, the structure and the number of parameters in models increase dramatically, making it very difficult to understand how models arrive at outputs from inputs. Additionally, the lack of standardized frameworks for explanation poses a challenge.

**Navigating Challenges in Dynamic Environments.** Machine learning models traditionally presuppose the stability of training data distribution. Yet, in practical scenarios, data distribution may evolve due to temporal, locational, and various external influences (Guo et al.; Samuel, E, Orna, Marcel, & Parijat; Subasri et al.; Yao et al.). Such dynamism necessitates model adaptability to prevent performance degradation over time. Challenges in dynamic environments arise from fluctuating external conditions and alterations in the data generation processes. For example, shifts in user behavior over time and changes in socio-economic conditions could impact data distributions. It is imperative for models to identify and adjust to these shifts, a capability that many current machine learning approaches lack (Ditzler, Roveri, Alippi, & Polikar; Hoens, Polikar, & Chawla; B.-D. S et al.; Sugiyama & Kawanabe).

To improve machine learning's effectiveness on individual entities and promote its deployment in significant decision-making processes, **models tailored to single individual objects** have been developed. Termed as personalized or customized machine learning, this strategy focuses on crafting models for specific entities (like individuals, corporations, or particular products), aiming to deliver tailored, precise solutions or services. The following section of this chapter will explore how these tailored machine learning models mitigate traditional approaches' limitations.

### 4.1.2 Hypothesis

The central hypothesis of this chapter is that machine learning models tailored to individual objects can significantly enhance accuracy, adaptability, and efficiency in specific application scenarios, outperforming general-purpose algorithms. By focusing on personalized customization, scenario-specific adjustments, and the integration of targeted

data augmentation techniques, these models can overcome limitations inherent in traditional machine learning approaches, such as low interpretability, limited flexibility in dynamic environments, and poor performance for minority or edge cases.

This hypothesis aligns with the broader thesis premise, which critiques the traditional emphasis on generalizability within the "Impossible Trinity" of machine learning. Instead, it posits that shifting focus towards scenario-based customization and adaptability will unlock greater potential for machine learning models, particularly in contexts with highly specialized requirements.

### 4.1.3 Defining "Individual Object"

Within machine learning and data science, an "Individual Object" generally denotes a distinct entity or point of observation in a dataset. This concept, applicable across various fields and applications, assumes meanings tailored to the context. In diverse settings, individual objects represent.

A patient in healthcare, with data spanning personal health records, genetic profiles, and physiological parameters.

A customer in retail and e-commerce, including purchase history, browsing habits, and preferences.

A user in social media analysis, with data on postings, interactions, and network connections.

An account holder in finance, encompassing transaction history, credit information, and risk preferences.

The term "Individual Object" encapsulates a broad notion, referring to a singular entity analyzed within a specific dataset or application. Defining individual objects is fundamental in machine learning, shaping the model's input, processing strategies, and ultimately, the personalized outcomes or decisions tailored to these entities.

### 4.1.4 Relevant Information for "Individual Object"

Custom machine learning models for individual objects require a deep understanding and analysis of the uniqueness and needs of each entity. The range of data covered should be extensive and in-depth, including aspects such as:

Basic Individual Information. Age, gender, geographical location, occupation, and other foundational data provide a basic framework for understanding the individual.

Historical Behavior Data. Past interactions, purchases, and usage records can help models understand an individual's preferences, habits, and needs across different application scenarios (Dahake, Mohare, & Somani; Y. Dong, Tang, & Zhang; Jagabathula & Vulcano; Sarker, Colman, et al.).

Social Network Data. If applicable, information on an individual's social networks, like friend circles, follow lists, and social interactions, can offer valuable insights into social preferences and influence (Amirali & Craig; M. D et al.; Le et al.; Sharad & D; Tianxi, E, & Ji).

Physiological and Psychological Data. In specific scenarios, such as health and medical fields, physiological data (e.g., genetic information, vital signs) and psychological data (e.g., psychological test results) are particularly important for custom models (Barenholtz, Fitzgerald, & Hahn; Carpenter; Dorraki et al.; Hagad, Moriyama, Fukui, & Numao, 2016; Magtibay, Fernando, & Umapathy).

Environmental and Situational Data. An individual's behavior and needs are often influenced by their environment and specific situations, making the collection of environmental information (e.g., weather, location features) and situational data (e.g., specific times, events) critical for building highly personalized models (Alexander, Dorota, Elisabeth, & N; Cosoli G et al.; Maedeh, Shahin, & Hojat; Max-Marcel, J, Gwendolyn, Christian, & Rüdiger; Ognjen, Jaeryoung, Miles, Björn, & Rosalind; Shihan et al.; H. Yu, Klerman, Picard, & Sano).

Device Usage Data. In technology-driven applications, patterns and preferences in the use of specific devices, such as smartphones and wearable devices, are important sources

of data reflecting an individual's technology affinity and lifestyle habits (Arivoli & Paul; Barbosa, Park, Yao, & Wang; Huoran & Xuan; Poghosyan, Pefkianakis, Le Guyadec, & Christophides; Stachl et al.).

Feedback Data. An individual's feedback on services, products, or content, including explicit feedback (e.g., ratings, comments) and implicit feedback (e.g., dwell time, click-through rates), is crucial for adjusting and optimizing personalized models (K. A; Hemadri & Lakshmish; Kota, Shuji, & Tatsuru; Marcos, M, José, Á, & M; Qian, F, G, & J; Ziang, Sarah, Bernd, Adam, & Jennifer).

By integrating these data types, a comprehensive and in-depth understanding of each individual object can be achieved, facilitating the development of more accurate and effective machine learning models tailored to them. The selection of relevant data types should be based on the actual conditions of the scenario. Moreover, it is imperative to strictly adhere to laws and regulations concerning data privacy and protection (Chuan-Kang; Paraskevi & Konstantinos; Macmillan R; K. M. S & R; Soumia, Gabriele, & Hüseyin; Venkateswara & Suman) to ensure the security and privacy rights of individuals are not infringed upon.

### 4.1.5 Characteristics of Individual Objects Data

The data pertaining to each individual object demonstrates several key characteristics during the customization process of machine learning models. These characteristics are crucial for designing and implementing efficient, precise personalized solutions. Understanding and leveraging these characteristics can significantly enhance model performance and user satisfaction. Below are the data characteristics and their utilization methods in model customization:

**High Personalization**

Characteristic. The data of each individual reflects its unique features, behaviors, and preferences (Fisher, Medaglia, & Jeronimus; Jagabathula & Vulcano; Katsikopoulos & Canellas; Provost; Reitinger, Wen, Mazurek, & Ur; Schramm; Taghikhah, Filatova, & Voinov). When an individual object is analyzed, the corresponding ontological data

possesses the highest information density and should be considered the most valuable source of information (A. G. J; Litzkendorf et al.; A. G. S & Mudasir; Shea–Budgell, Kostaras, Myhill, & Hagen; Theodoros, X, L, & D).

Utilization Method. In model design, it is essential to fully consider all stages of model construction, utilizing individual information in as many stages as possible, such as data processing, algorithm design, and model evaluation. This enables the optimization direction of the model to be adjusted based on individual information.

**Dynamic Variation**

Characteristic. The behavior, state, and environment of an individual may change over time (Razmi & Nassar; Tennenholtz, Merlis, Shani, Mladenov, & Boutilier; F. Tian et al.; Rui Wang, Shen, Tino, Welchman, & Kourtzi).

Utilization Method. Implement dynamic learning strategies, enabling the model to adapt to changes in individual behavior. This may include using online learning algorithms and regularly updating the model to reflect the latest data. This characteristic also demands that the entire process of model should have strong repeatability and minimal resource consumption. The entire process includes design, training and deployment. The applicability of the model can only be ensured if it can keep up with the changes in the individual objects.

**Multidimensionality**

Characteristic. The data of individual objects usually encompasses multiple dimensions, such as social networks, behavioral logs, physiological information, etc. Even for features within the same domain, the scale and distribution differences among them can pose many challenges to data analysis (P. A & J; Fan, Han, & Liu; Kehrer & Hauser; J. Li & Liu; Santra & Bhowmick, 2017).

Utilization Method. For data belonging to different types, consider adopting multimodal learning methods to integrate data from various sources for a more comprehensive individual profile (Chua; Farnadi, Tang, De Cock, & Moens; Farseev, Nie, Akbari, & Chua; Kulvinder & et al.; L. Zhang, Fu, Jiang, Bao, & Zeng, 2018). This helps

the model understand individuals from multiple angles and improves the accuracy of predictions or recommendations. For data of the same type, the model needs to employ data processing techniques like feature engineering and data normalization to facilitate effective model guidance during training. Moreover, the reality of having multidimensional and even multiple data types requires that models customized for individual objects consider the data situation of individual objects in their structural design (Z. Jiang, Wen, Han, Tang, & Xiong; Kroll & Soldan; Streit, Schulz, Lex, Schmalstieg, & Schumann), using the most appropriate structure to process specific data.

**Sparsity**

Characteristic. For some individuals, part of the data may be very sparse, especially in the early stages. This is particularly the case when the individual object data is in a sparse area of the sample space, indicating that the individual object itself is relatively rare.

Utilization Method. Pre-trained models or transfer learning techniques should be introduced to compensate for the lack of data by using data from other similar individuals or domain knowledge. Additionally, techniques to augment data, such as data imputation and Generative Adversarial Networks (GANs), can be employed (Arantes, Vogiatzis, & Faria; Fabio & C; Meor Yahaya & Teo; Manjunath S, Aitzaz, Jeff, & Stan; Shodamola, Qureshi, Masood, & Imran; Shorten & Khoshgoftaar). For the model to be effectively customized for any individual object, it must possess the capability to process specific objects. The performance of general models has already been validated across a broad statistical spectrum for handling the majority of common individuals (Fugard & Stenning; J. Diaz, Yeh, & de Leon; Mori et al.; Nikolikj, Kostovska, Cenikj, Doerr, & Eftimov). Customizing models for individual objects is intended to fill the ecological niche that traditional models cannot cover for special individual objects. Arguably, the ability to process specific objects is the most fundamental value of models customized for individual objects.

**Privacy Sensitivity**

Characteristic. Individual data often contains sensitive information that requires strict privacy protection (Anant & Prasad; Filippo; Izgi; Prakash M & G; Min & Zuosu; Pant).

Especially when customizing based on individual objects, richer data can be accessed without de-identification, demanding utmost caution during data processing and transmission (Arvind, Joanna, & E; Junhyoung & K; Luc, J, & Y; A. T. Neil & M; Garfinkel S; Tzvika et al.).

Utilization Method. Privacy-preserving techniques, such as differential privacy and homomorphic encryption, are used to ensure individual privacy during data analysis and model training (Ahamed & Ravi; Aziz, Banerjee, Bouzefrane, & Le Vinh; Smajić, Grandits, & Ecker; Tanuwidjaja, Choi, & Kim, 2019; Upadhyay, Kumar, Roy, & Rawat; H. Zheng, Hu, & Han). A more acceptable approach for users is to run the model training and final deployment on the individual's personal device, which can operate offline (without a network connection), thereby eliminating the risk of information leakage from the source. If such demands are to be met, the entire model construction process must be lightweight.

**Imbalance**

Characteristic. In some applications, individual object data may be imbalanced in terms of category distribution, such as in medical diagnostics, where samples of certain diseases may be far less than others (D. Dong & Shaowen; F, Suhel, Firuz, & Amanda; Ibomoiye & Yanxia; K. M. Sunil, Sudarshan, & Vipul; Tzu-Hsien, Zhan-Yi, Yu-Huai, & Min; Varsha; Weixian, Rong, Yang, Ruixuan, & Weishi). Or due to the low incidence of diseases, the sample size of diagnosed patients is much smaller than that of the healthy population.

Utilization Method. Employ techniques for handling imbalanced data, such as oversampling the minority class, undersampling the majority class, or applying specially designed loss functions to improve the model's recognition ability for minority classes (Amelia, Hasibuan, & Pane; Buda, Maki, & Mazurowski; Md, S, Shuxiang, & D; Mohammed, Rawashdeh, & Abdullah; D. N, Chadaga, Singh, & N; Thumpati & Zhang; Tyagi & Mittal, 2019; Wibowo & Fatichah). If it is not possible to obtain knowledge-based optimization strategies during the data processing phase, the model must be designed to automatically handle imbalanced data.

By considering these characteristics comprehensively and adopting corresponding

strategies, the potential of individual data can be maximized during model customization, providing each user with more accurate and satisfactory services.

### 4.1.6 The Relationships Between Individual Objects

The relationships among individual entities significantly influence the customization process of models. Grasping and dissecting these connections and variances can markedly elevate the model's efficiency and precision, particularly within the realm of personalized service or product offerings (González & Tansini, 2022; Maxim, F, & Arnon; Nedungadi & Smruthy, 2015; Valentina, A, & M; Yaghtin & Mero). Below are various relationships that might exist among individual entities, along with an exploration of how these interactions facilitate model customization.

**Similarity**

Description of Relationship. Individuals may share similarities across specific dimensions or attributes, such as users with analogous purchase histories showing interest in comparable products within recommendation systems (Chantima & S; L. Chen, Minjia, Mahboob, Saleh, & Y; D. M & S; Masahiro, Hidetaka, & Takashi; Masahiro, Janmajay, et al.). Utilization in Customization. Analyzing the similarities among individuals allows for the application of techniques like collaborative filtering to suggest items of potential interest (Bansal & Jain; Chowdhury & Sinha; Praveen Kumar, Gupta, Rao, Bhavsingh, & Srilakshmi). Additionally, this analysis of similarity can aid in transfer learning, enabling the partial transition of learning outcomes from one individual to another akin entity.

**Social Relationships**

Description of Relationship. Social relationships can bind individual entities together, whether they are friends, family, or colleagues (Manuja & Bhattacharya; Mukamakuza, Sacharidis, & Werthner; Shaikhah & Julita; T. Zhao, McAuley, & King). Utilization in Customization. Analyzing social networks can reveal the influence of society on individual preferences. Models can exploit these potential influences to enhance the relevance and personalization of recommendations, such as suggesting content favored by one's social group.

**Group Affiliation**

Description of Relationship. Individuals may be categorized into various groups based on distinct traits or attributes, such as occupation, hobbies, or lifestyle choices. Utilization in Customization. Recognizing an individual's group affiliations aids models in comprehending the collective needs and preferences, thus incorporating group characteristics into customization to offer more apt services (Dehghani, Azarbonyad, Kamps, & Marx; Ortega, Bobadilla, Hernando, & Gutiérrez; Purushotham & Jay Kuo, 2015; Zeng & Chen, 2013).

**Competitive or Adversarial Relationships**

Description of Relationship. In certain scenarios, individuals might engage in competitive or adversarial dynamics, such as within gaming or auction environments (Daniel, Brenton, & Mino; Lisy, Jakob, Tozicka, & Pechoucek; Villareale, Harteveld, & Zhu; Ye et al.; Zuckerman, Kraus, Rosenschein, & Kaminka). Utilization in Customization. Understanding these dynamics enables models to anticipate individual strategies or behaviors, tailoring more effective responses or recommendations.

The scrutiny of variances among individuals proves invaluable for tailored model development, enhancing precision by capturing the unique needs and preferences of each entity, boosting the model's ability to discriminate between when general knowledge applies and when specific individualized attention is warranted, thereby refining customization without compromising on generalization (Monjurul Hasan & Lu; Hecksteden et al.; Kenney, Jimeng, Jianying, & Fei; Luo, Nikolopoulou, & Gevertz; Peter & S; Wright & Woods). Moreover, this understanding facilitates more strategic resource distribution, particularly in targeting marketing efforts towards demographics most likely to yield positive responses.

In essence, the examination of the intricate web of relationships and differences among individual entities stands as a cornerstone for developing models that are not only efficient and precise but also capable of significantly enhancing user experiences while optimizing both system performance and resource allocation across various dimensions.

### 4.1.7 Leveraging Individual Objects Data Effectively

When customizing models for a specific individual, it is crucial to fully utilize the data of that solitary entity. Here is a comprehensive strategy illustrating how to exploit individual data from various perspectives to achieve highly personalized model customization.

**Understanding Individual Characteristics Thoroughly**

Comprehensive Data Collection. Gather data from multiple sources mentioned earlier, such as basic information, behavioral data, social network information, etc., to obtain a thorough understanding of the individual.

Feature Engineering. Meaningful information is extracted through feature engineering to transform raw data into a form that can be utilized by models. Considering the uniqueness of individuals, feature engineering may include customised feature selection or construction.

**Analyzing Behavior Patterns**

Behavior Analysis. Use historical behavior data to analyze individual preferences and habits, including frequent activities, preferred time slots, and reactions to specific events.

Dynamic Adaptation. Design models that consider the dynamic changes in individual behavior, employing algorithms capable of adjusting over time, such as online learning or incremental learning methods, to accommodate changes in individual preferences.

**Utilizing Social and Group Information**

Social Network Analysis. If data is available, analyze the individual's social network to predict individual preferences using social relationships and group behaviors.

Group Feature Integration. While maintaining individual customization, consider group characteristics as auxiliary information to enhance the model's predictive capability.

**Addressing Data Sparsity and Privacy Issues**

Data Augmentation. For individuals with sparse data, employ data augmentation

techniques, such as synthetic data generation or using information from similar individuals for data imputation.

Privacy Protection. Strictly adhere to data privacy protection principles in all processing steps, employing differential privacy and data anonymization to prevent individual data from being disclosed.

**Implementing a Feedback Loop**

Collecting Feedback. Implement mechanisms to collect individual feedback on model outputs, including explicit feedback (such as ratings and comments) and implicit feedback (such as click-through rates and usage duration).

Model Iteration. Continuously adjust and optimize the model using collected feedback to ensure the model outputs meet the evolving needs of the individual.

Through such a strategy, not only can individual data be fully leveraged to achieve highly custom models, but it also allows for the adaptation to changes in individual needs while protecting individual privacy, offering more accurate and personalized services or products. The key to this methodology lies in meticulous data analysis, a deep understanding of individual characteristics, and the continuous optimization and iteration of model performance.

## 4.2 The Case for Research

### 4.2.1 A Brief Description of Hepatitis C Disease

Hepatitis C is an undetectable silent killer, a serious disease that is slowly progressive and potentially carcinogenic, and can remain latent in the body for 10–20 years (Alter, 1997; Poynard, Yuen, Ratzin, & Lai, 2003). Typically, only about 30% of patients with hepatitis C virus infection can recover spontaneously within six months, and 70% of patients turn into chronic viral infection (Scheuer, Ashrafzadeh, Sherlock, Brown, & Dusheiko, 1992). The hepatitis C virus is extremely stealthy, and WHO estimates that only

about one in five of the more than 50 million people living with hepatitis C worldwide are aware that they have the disease, with an underdiagnosis rate of up to 80% (Organization, 2017). In the early to mid-stages of hepatitis C infection, there are usually no obvious signs and symptoms. Patients may experience dizziness and weakness and poor sleep, which can easily be confused with fatigue caused by work or study (Seeff, 2002). As a result, many patients are often found to have hepatitis C when they are examined for other diseases, and some patients are even found to have hepatitis C when cirrhosis or liver cancer is detected. It is because of this stealthy nature that the damage caused by hepatitis C is chronic and progressive. The hepatitis C virus replicates primarily in the liver cells and damages them (Lauer & Walker, 2001). Over time, liver cells in the body will continue to develop inflammation, degeneration and necrosis. There is no vaccine to prevent hepatitis C, so people at risk can only be diagnosed and treated for hepatitis C in a timely manner by taking the initiative to get tested for the hepatitis C virus at the hospital (MacArthur et al., 2014). Although hepatitis C is dangerous, only 1 ml of blood is needed to test for infection with the virus. Once diagnosed, there is no need to panic, as more than 95% of patients with hepatitis C can be cured with standardized and systematic treatment (Burstow et al., 2017; Ghany, Strader, Thomas, & Seeff, 2009; Kohli, Shaffer, Sherman, & Kottilil, 2014; Strader, Wright, Thomas, & Seeff, 2004).

However, the greatest difficulty in the prevention and treatment of hepatitis C disease is that most patients do not know that they have hepatitis C. The mainstream diagnostic tools for hepatitis C are: 1. Liver function tests (LFTs), which assess liver disease from liver-related metabolites (Gowda et al., 2009; Limdi & Hyde, 2003; Thapa & Walia, 2007). 2. Hepatitis C antibody tests, which clarify whether the body is infected with the hepatitis C virus. If the test result is positive, it indicates that the patient is currently infected with hepatitis C or has previously been infected with hepatitis C (McGibbon, Bornschlegel, & Balter, 2013; Tang et al., 2017). 3. Hepatitis C virus RNA test, this test can effectively determine how long the infection has been present and also how much of the virus is present in the patient's body (Al Olaby & Azzazy, 2011; Pawlotsky et al., 2000). 4. Liver puncture or ultrasound: this is the main way to determine the severity of the liver disease. Generally speaking, if the disease is serious or has a long duration, these two tests should

be used to analyze the progress of the liver disease, which is also the key to the current treatment process for patients who are diagnosed (Caturelli et al., 1996; Kalambokis et al., 2007).

Among these tests mentioned above, only liver function tests are easy to perform at regular checkups and have high marginal utility (LFTs can be used to analyze many diseases related to the liver). Antibody and RNA tests are more targeted and less prevalent in general health care facilities, and are relatively costly and not conducive to mass adoption. Puncture tests or ultrasounds are generally used to detect the progression of disease in patients with confirmed disease and are not suitable for making early disease diagnosis. This is why making good use of the data from liver function tests has become an effective means of identifying hepatitis C patients earlier.

It is due to the characteristics of hepatitis C: high health impact, large population involved and expensive RNA testing. Customised analysis of each potential patient using only liver function test data can be performed at a very low cost and with a high degree of accuracy.

### 4.2.2 Dataset and Preprocessing

To cope with the shortcomings of traditional detection means, difficult, costly, and time-consuming, this chapter tries to diagnose hepatitis C status through the use of blood biomarkers (O. A, Scott, & T; Arca-Lafuente, Martínez-Román, Mate-Cano, Madrid, & Briz; Mukherjee et al.; Shahid et al.; Shenge & Osiowy; Villar et al.). The Hepatitis dataset from UCI machine learning repository was selected to show the effectiveness of the custom algorithm (Alqaissi, Alotaibi, & Ramzan; Dixon et al.; Smriti Mishra, Kumar, Tiwari, & Ranjan; Natrayan, Kamal, Manivannan, & Sunil). This dataset involves blood biomarkers used to detect the hepatitis C virus and contains laboratory values for 615 blood donors and hepatitis C patients, as well as demographic values such as age. The target attribute for classification is the category (blood donors vs. Hepatitis C). And there are 14 attributes.

Ethical Considerations. The data involved in this chapter are all data obtained from publicly available sources (Lichtinghagen & Hoffmann) and have been properly cited

according to the data publisher's requirements. Some of the data related to case information of some patients, where information related to identity has been removed or desensitized by the data publisher so as not to reveal the privacy of the patient.

But obviously, accuracy of previous work is not sufficient for medical applications, so more advanced tools are needed to analyze the data (Akella & Akella; Doyle, Leavitt, & Rigg; Farrag, Kamel, & El-Baraky; Frias et al.). This section will also analyze this data using some of the most popular algorithms in the field of machine learning classification nowadays, in order to compare the advantages of the proposed approach in this chapter.

Exploratory Data Analysis. Perform basic evaluation checks on the data by calling the functions of pandas (McKinney, 2011), NumPy (Oliphant, 2006a). Load the training and test sets and briefly browse the data: head() +.shape(), get familiar with the relevant statistics of the data by.describe(), get familiar with the data types, view the corresponding data column names, and NAN missing information by.info(). View the presence of NAN for each column to determine missing and abnormal data. Have a preliminary perception of the data. Some basic information and analysis of the data are shown in Table 1.

Handling of abnormal data and missing values (Alabadla et al., 2022). Each kind of data has its own actual meaning behind it. When the data value exceeds the normal range or is a meaningless expression, it needs to be adjusted or supplemented in a targeted way. The dataset used here was reviewed by the medical staff, and there were no obvious abnormal values. As analyzed in 3.2.1 (a), the user of the data can pre-process the data based on his or her own knowledge and experience. The effectiveness of data processing at this point is largely determined by human factors. In this study, manual supplementation of flawed data was avoided as much as possible in order to minimize human influence. For patient data with missing values in the dataset, this study chose to remove them. The processed data samples have the following features from x1 to x12: Age, Sex, ALB, ALP, ALT, AST, BIL, CHE, CHOL, CREA, GGT, and PROT. Each sample has a label y1 with 1 and 0 for disease or absence of disease, respectively.

Table 1. Statistics for Each Feature of the Dataset.

| feature | mean | median | STD | STD | range |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| Age | 47.41 | 47 | 0.405 | 10.06 | [19,77] |
| Sex | 0.55 | 1 | 0.020 | 0.50 | [0,1] |
| ALB | 41.55 | 41.9 | 0.243 | 6.01 | [0,82.2] |
| ALP | 66.29 | 65.3 | 1.134 | 28.11 | [0,416.6] |
| ALT | 28.40 | 23 | 1.027 | 25.47 | [0,325.3] |
| AST | 34.79 | 25.9 | 1.334 | 33.09 | [10.6,324] |
| BIL | 11.40 | 7.3 | 0.793 | 19.67 | [0.8,254] |
| CHE | 8.20 | 8.26 | 0.089 | 2.21 | [1.42,16.41] |
| CHOL | 5.28 | 5.29 | 0.053 | 1.31 | [0,9.67] |
| CREA | 81.29 | 77 | 2.006 | 49.76 | [8,1079.1] |
| GGT | 39.53 | 23.3 | 2.204 | 54.66 | [4.5,650.9] |
| PROT | 71.93 | 72.2 | 0.247 | 6.13 | [0,90] |

Note: STE is the Abbreviation for Standard Error and STD is the Abbreviation for Standard Deviation (Lichtinghagen & Hoffmann).

The feature selection process in filtered and wrapped feature selection approaches is explicitly decoupled from the learning training process, which allows for more accurate correlation analysis. As the name suggests, correlation analysis involves looking at how closely related two variables are by analyzing them together. Correlation analysis can only be carried out if there is some sort of link or probability between the associated elements. Carl Pearson, a well-known statistician, developed the correlation coefficient (Asuero, Sayago, & González, 2006). The correlation coefficient is a statistical measure of the degree to which two variables are related to one another. By multiplying the two deviations from their respective means, the product-difference approach yields the correlation coefficient; this method is especially useful for calculating the linear single correlation coefficient. Use of the Seabon (Waskom, 2021), a Python data visualization library based on matplotlib (Tosi, 2009), visualization package to create a scatter plot of the correlation analysis matrix. The correlation analysis revealed that the x6 feature (AST, Aspartate aminotransferase) is very important for the final label. There are also x7 (BIL, Bilirubin), and x11 (GGT, Gamma-Glutamyl Transferase) that contribute to some extent. There is also a clear correlation between features x3 (ALB, Albumin) and x12(PROT, Protein). Visualization of the relationship between digital features based on correlation analysis and several common means of preliminary data analysis were also used to gain a preliminary understanding of the data, but no modifications were made to the data at this stage.

There seems to be a lot of noise/outliers (Gupta & Gupta, 2019). Some data engineers choose to remove outliers at a fixed rate and then normalize the data to facilitate analysis (Atla, Tada, Sheng, & Singireddy, 2011). However, considering that this is a medical dataset, all the data is kept in this case to ensure that the data can cover more rare cases. The main purpose of feature engineering is to improve the performance of machine learning by transforming data into features that better represent the underlying problem. Outliers are processed to remove noise and features are constructed to enhance the representation of the data. In order to better enable the use of machine learning models by people who do not have a rich industry background, no additional knowledge is introduced in this case to perform complex processing of the data.

Because of the limited amount of data in the medical dataset, each patient's data information is very precious. Therefore, in order to make full use of this information, the training set is divided in a special way. Each time a specific patient is analyzed, this chapter defines the patient's laboratory results as a separate test set and assign all the remaining data to the training set. In other words, each patient to be analyzed, in what follows in this chapter, is considered as an **individual object**. Whenever a patient changes, the training set changes as well. This is designed to mimic the actual scenario of hospital diagnosis, i.e., for a new patient seeking medical treatment, all the previously saved analysis data is used as the training set to train the model for the new patient.

### 4.2.3 Related Work

Although this chapter is a study of the diagnostic issues of hepatitis C, it is essentially an analysis based on medical data already collected and does not involve relevant medical-related knowledge. Therefore, in this section, this research will not analyze the virology of hepatitis C and disease-related knowledge, but mainly summarize the existing data analysis tools for the disease and their effects. In this section, we will discuss: 1. the development of structured data processing in the field of machine learning; 2. the customization and lightweighting of traditional models for specific application scenarios to make them easier to use; and 3. the progress of studies using the same dataset.

**Methods of Processing Structured Data**

1) Gradient Boosted Decision Tree

The field of structured data (i.e., tabular data) has historically been dominated by conventional machine learning algorithms like Gradient Boosted Decision Tree (GBDT) (T. Chen & Guestrin, 2016) due to their better performance (Shwartz-Ziv & Armon, 2022). Scientists and businesses alike rely heavily on several GBDT algorithms, the most popular of which being XGBoost, LightGBM (Ke et al., 2017), and CatBoost (Prokhorenkova, Gusev, Vorobev, Dorogush, & Gulin, 2018). A scalable gradient boosting tree technique, GBDT produces state-of-the-art results on numerous tabular datasets, and XGBoost is one of the most prominent implementations of GBDT. The process known as "gradient boosting" builds new models using the residuals of older models to produce more accurate predictions (Badirli et al., 2020; Y. Zhao, Chetty, & Tran, 2019). XGBoost's foundation is the same as GBDT's, but it is been improved upon. For example, the second-order derivative makes the loss function more accurate; the use of regular terms to avoid tree overfitting, etc.

2) Deep Neural Models

Since deep neural networks have been so successful in image recognition, numerous recent research have extended deep learning to the area of tabular data, with the goal of improving the performance of tabular data by introducing novel neural architectures (Borisov et al., 2022; Huang, Khetan, Cvitkovic, & Karnin, 2020; Klambauer, Unterthiner, Mayr, & Hochreiter, 2017). Based on the deep learning ideas these models draw from, the models can be classified into two categories.

Attention-based models. Given the novel route taken by attention-based models in deep learning, several researchers have experimented with attention-like modules in tabular deep networks. Two types of focus have recently been proposed: inter-sample attention, where characteristics within a single sample interact, and intra-sample attention, where individual data points make advantage of row-level or sample-level interactions. (Arik & Pfister, 2021; Somepalli, Goldblum, Schwarzschild, Bruss, & Goldstein, 2021).

Differentiable trees. The series of work presented here seeks to make decision trees differentiable because of the impressive results obtained by decision tree ensembles when applied to tabular data. Due to their lack of differentiability and gradient optimization, classical decision trees are limited in their use in some specific application scenarios. Fortunately, recent research has found a solution to this issue: by making tree functions and tree routing differentiable by smoothing the decision functions in the internal tree nodes differentiable (Kontschieder, Fiterau, Criminisi, & Bulo, 2015; Popov, Morozov, & Babenko, 2019). But even with the improvement of these new approaches and the combination of them, it is still difficult for deep neural models to outperform traditional GBDT across the board in structured data.

**Customization and Lightweighting of Complex Models**

With the rapid accumulation of data (Hilbert, 2016; J. Qiu, Wu, Ding, Xu, & Feng, 2016), a variety of all-encompassing datasets have been built (Bojar et al., 2014; J. Deng et al., 2009; T.-Y. Lin et al., 2014), the differences between data and compatibility issues were ignored. This neglect leads to the difficulty for complex models for complete scenarios to perform consistently on all problems (C. J. Cai et al., 2019; Harrison et al., 2020), there will always be particular problems that are substantially off in prediction, and there will always be images that cannot be correctly classified. This leads to the fact that if one wants to apply large proven models to specific particular datasets, that is, to adapt the original models to specific problems, this is not easy to achieve. In the field of problem-based machine learning research, there has been a minimal exploration of this.

Some researchers (Dai, Jin, Xue, Yang, & Yu, 2009; Z. Deng, Choi, Jiang, & Wang, 2014; C. Tan et al., 2018a; Torrey & Shavlik, 2010; Karl Weiss, Taghi M Khoshgoftaar, & DingDing Wang, 2016) discusses how existing complex models can be tailored to specific problems, making the original model better applicable to specific datasets using transfer learning. Since traditional mature neural networks are large and bloated, some researchers (G. Chen et al., 2017; J. H. Cho & Hariharan, 2019; Gou et al., 2021; Phuong & Lampert, 2019; Yim et al., 2017) compress the parameters of the existing model by employing knowledge distillation and model simplification to achieve the effect of improving the

speed of computing. There also are several scholars who proposed some tricks for data augmentation (Y. Jiang et al., 2019; Mikołajczyk & Grochowski, 2018; Shorten & Khoshgoftaar, 2019; L. Taylor & Nitschke, 2018; Jason Wang & Perez, 2017), which can make the model improve the accuracy of analysis in specific scenario. However, these solution ideas are still rarely discussed for very specific individual problems, and this chapter will try to fill the gap and demonstrate the feasibility.

**Hepatitis C Disease Diagnosis Using the Same Dataset**

In the field of medical diagnostics, machine learning has been showing its capabilities since very early on. Back in 2017, Hashem et al. compared several ways to predict hepatitis C using blood markers, yielding a best accuracy rate of 66.3% to 84.4% (Hashem et al., 2017). In 2018, Hoffmann et al. collected and organized the dataset used in this chapter, several medical researchers analyzed the data through a tree model, yielding an accuracy rate of best 75.3 (Hoffmann, Bietenbeck, Lichtinghagen, & Klawonn, 2018). This dataset was donated to the UCI Machine Learning Repository in June 2020 (Lichtinghagen & Hoffmann). After that, Chicco and Jurman used the dataset to perform Ensemble Learning on the AST/ALT ratio to achieve a 95.4% accuracy rate on whether the disease was present or not (Chicco & Jurman, 2021). Chawathe et al. achieved a 95% accuracy rate and 89% recall rate by fusing multiple models. But for specific applications in medical diagnosis, all this needs to be enhanced (Chawathe, 2020). We need to make every effort so that all patients are accurately identified and all healthy patients can be correctly classified without additional biopsies.

## 4.3 A Machine Learning Model Framework Tailored to Each Potential Patient

In order to make the best use of the collected data, a powerful tool such as machine learning is natural. However, the current direction of machine learning is deep learning, which relies on a large number of datasets, which contradicts the small amount of medical-related data accumulated today. Borisov et al. points out that deep learning methods have a major disadvantage in the processing of structured data (Borisov et al., 2022), and the

performance of deep learning models with huge numbers of participants is even far behind some commonly used tree models (Shwartz-Ziv & Armon, 2022). And there are also obvious ethical issues with today's machine learning models when dealing with medical-related problems, as they are judged by their average performance on the validation set. Perhaps the model can perform well on average, but who wants to be the "unlucky patient" who is misjudged by the model? Every data sample that is processed by the model is closely related to a patient. The disease diagnostic model is not just discussing the categorization of this data sample, but will actually affect the future of a flesh-and-blood real individual. In order to overcome the above ethical issues, the primary pursuit of a custom model for the selected target patient is the highest possible degree of accuracy. It is important not only to aim for an overall average performance of the model, but also to ensure that the worst performance in each case is acceptable.

In this chapter, a machine learning model for hepatitis C diagnosis customized for each patient is proposed. The major difference from the traditional model is that the data of the patient to be diagnosed is incorporated into the training process. The comparison of the customized solution and traditional machine learning is shown in Figure 12. With the help of richer information, the model achieves better accuracy and can correctly categorize almost all patients.

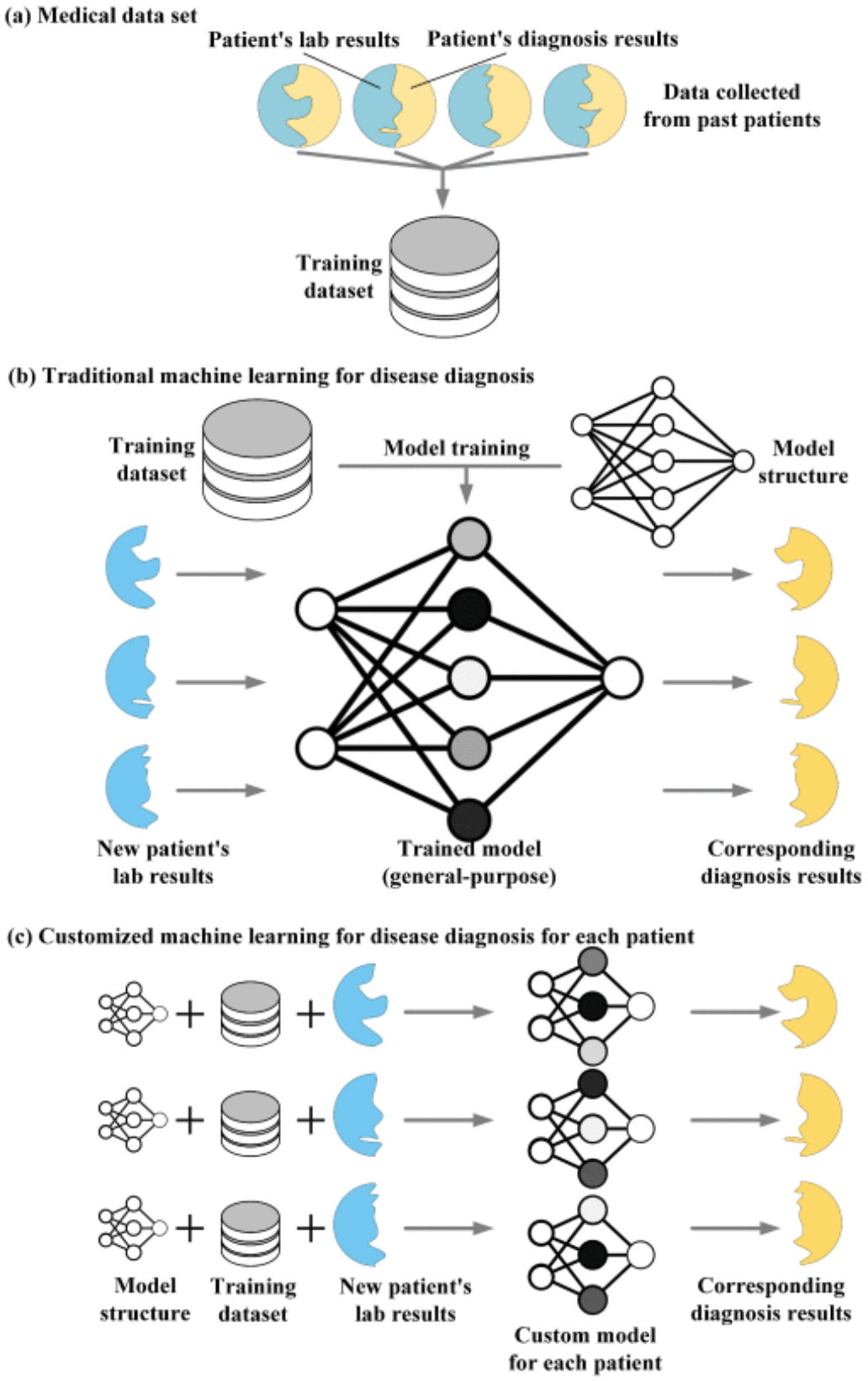



*Figure 12. Comparison of the customized solution and traditional machine learning.*

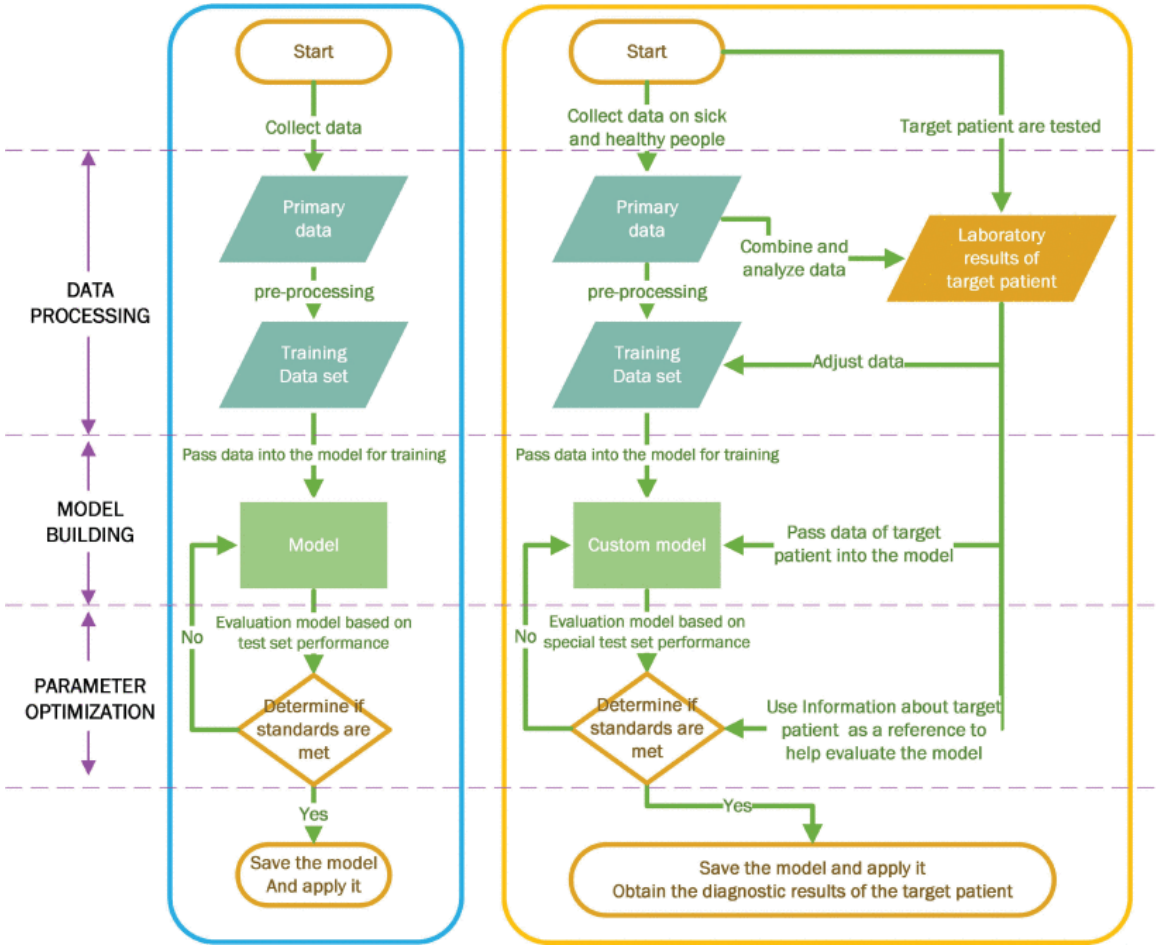



*Figure 13. The framework of the custom algorithm.*

Note: The yellow box is the acquisition process of the traditional machine learning model, and the blue box is the acquisition process of the custom machine learning model.

Guided by the above analysis and chapter three, the algorithm proposed in this chapter implements model customization for patients in three stages. 1) data processing stage: targeted sample augmentation. 2) model structure design stage: patient data are skillfully passed to the model. 3) hyperparameter optimization stage: model performance under different hyperparameters is judged by new evaluation criteria. This chapter calls an individual patient who needs a disease diagnosis a “target patient (individual object)”. Each patient’s laboratory results can be considered a sample, and a medical dataset will have a very large number of samples.

The framework of the algorithm is depicted in Figure 13, which is divided into three

major parts, they are data processing, model building, and parameter optimization. The yellow box on the left is the acquisition process of the traditional machine learning model, and the blue box on the right is the acquisition process of the custom machine learning model proposed in this chapter.

## 4.4 Specific Solutions

The proposed specific approach is explained in the following three levels: data processing, model structure design, and hyperparameter optimization.

### 4.4.1 Targeted Data Augmentation

This chapter proposes to adjust the proportion of training samples (targeted data augmentation). The operation of this part is shown in Figure 14.

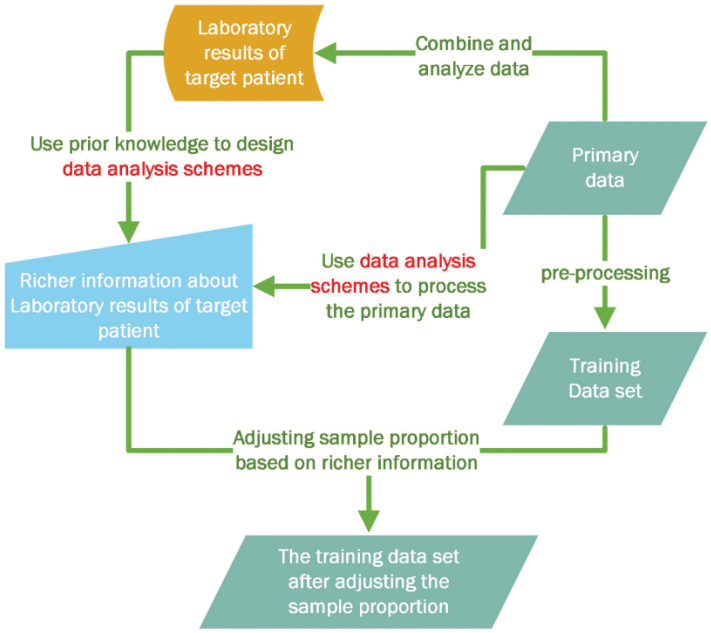



*Figure 14. The framework of the custom algorithm.*

EDA (Exploratory Data Analysis) (Behrens, 1997; Dodge, 2008) is an essential part of machine learning and is the first step that starts after acquiring data. In this process, the original data is explored with as few a priori assumptions as possible, summarizing the structure of the data and presenting specific patterns. For a single feature, the data engineer always expects that the variables under that feature can be uniformly distributed or

normally distributed within the data. For the whole sample space, the data engineer always expects that each data point can be uniformly distributed in the sample space (it means that the probability (density) corresponding to each sample point in the whole sample space is equal) (Milo & Somech, 2020). This is because imbalanced data can seriously affect the model's effectiveness and even affect the judgment of the model, good or bad. The accuracy of the model is very high for the high proportion categories, and the deviation of the prediction is exceptionally high for the low proportion categories. Nevertheless, the researcher naively thought to get a good model because the higher proportion categories had a more significant effect on the loss and metric (Sahoo, Samal, Pramanik, & Pani, 2019).

However, in a dataset containing a large number of samples, there is always only limited sample data in the region that should be focused on. If a laboratory result for patients who need to be diagnosed is introduced in the original sample space, the percentage of samples in the training set that are similar to the target patient is tiny. In order to improve the accuracy of the model for the target patient, the proportion of training samples can be adjusted by targeted data augmentation (Alwosheel, van Cranenburgh, & Chorus, 2018). In the case of the disease diagnosis problem discussed in this chapter, to make the custom model more accurate for the target patient, what is done is to reduce the level of attention to the cases that differ significantly from the target patient and pay extra attention to the cases that very similar to the target patient. This allows the model to be more sensitive in identifying potential patients and also allow the model to make correct judgments when faced with healthy cases (S. C. Wong, Gatt, Stamatescu, & McDonnell, 2016).

The specific operation is as follows: 1. Find several samples from previously collected case datasets closest to the target patient in the whole sample space; 2. Increase the number of these similar samples by a specific method to occupy a more significant proportion of the entire sample space (Tanner & Wong, 1987; Van Dyk & Meng, 2001). That is, increasing the sample density in the vicinity of a specified individual object in the sample space.

After determining the idea of targeted data augmentation, two questions arise: 1. how to describe the similarity between samples in the sample space, that is, how to determine that the laboratory results of two patients are more similar; 2. how to expand the number of similar samples by what means. In machine learning and data mining, the concept of "statistical distance" is often introduced to describe the magnitude of differences between individuals and thus evaluate the similarity and class of individuals. Depending on the characteristics of the data, different measures can be used. In general, to define a distance function $d(x, y)$, the following criteria need to be satisfied (Dodge, 2003):

1. Non-negativity:

$$d(x, y) \geq 0 \tag{1}$$

2. Identity of indiscernible:

$$d(x, y) = 0 \text{ if and only if } x = y \tag{2}$$

3. Symmetry:

$$d(x, y) = d(y, x) \tag{3}$$

4. Triangle inequality:

$$d(x, z) <= d(x, y) + d(y, z) \tag{4}$$

Based on these criteria, the Euclidean distance (Liberti, Lavor, Maculan, & Mucherino, 2014) was selected, Mahalanobis distance (De Maesschalck, Jouan-Rimbaud, & Massart, 2000), Chebyshev distance (Klove, Lin, Tsai, & Tzeng, 2010), Minkowski distance (Groenen & Jajuga, 2001), and Bhattacharyya distance (Choi & Lee, 2003) as alternative options. After a comparison test, the Mahalanobis distance was finally chosen as the criterion to describe the sample similarity. Its most prominent advantage is modifying the traditional Euclidean distance, which corrects the problem of inconsistent and correlated scales of each dimension in the Euclidean distance. It can genuinely reflect the similarity relationship between samples without the constraints of dimensional scales. Other distance criteria in the comparison experiments were more or less influenced from the complex

dimensions, resulting in calculated distances that did not satisfy the needs of subsequent experiments. To increase the number of few samples in the training set that are similar to the target patient to achieve sample balancing, the SMOTE (Synthetic Minority Over-sampling Technique) (Chawla et al., 2002) algorithm was chosen after comparing various methods for adjusting the sample proportions. The SMOTE method is an interpolation-based method that synthesizes new samples for small sample classes. By calculating the Mahalanobis distance between the sample points in the training set and the target patient, a certain stem of samples that are most similar to the target patient is oversampled. The result of this processing is shown in Figure 15. The figure shows a two-dimensional (feature) sample space in which the yellow triangle represents a positive sample and the blue pentagon represents a negative sample. The target patient is to categorize the green squares (target samples) in the sample space. After the Targeted data augmentation process, the samples in the original sample space are targeted augmentation (which can be interpreted as simply copying the samples to increase the weights). The augmentation results in augmenting the samples that are more similar to the target samples and paying more attention to the samples that are more similar.

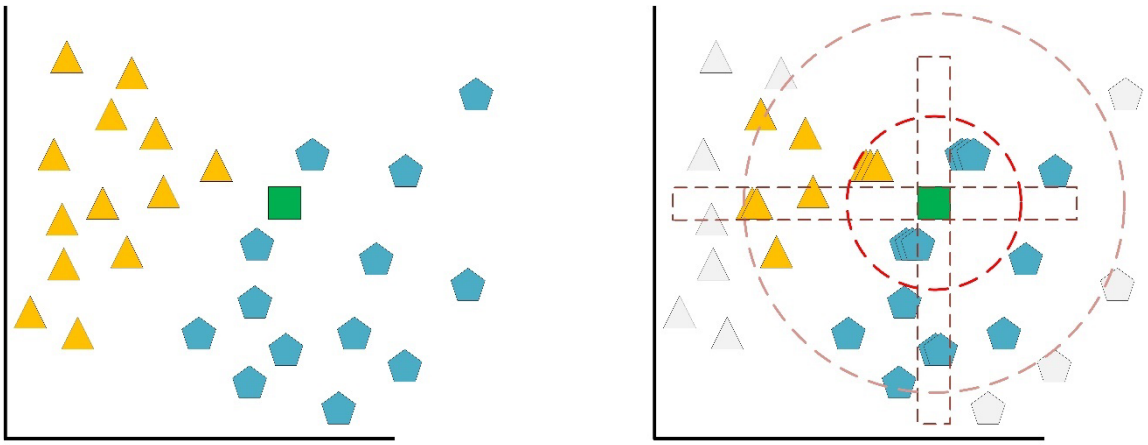


*Figure 15. Targeted data enhancement effect comparison chart*

The data before processing is defined as $D$ shown in equation (5), where there are $n$ samples in total, and each sample is differentiated by $i$. The features (dimensions) are $d$ in total and are distinguished by $k$. The output labels (dimensions) are $l$ in total and are distinguished by $o$. So, write $X$ and $Y$ in the form of separate matrices as Equation (6).

$$D = \left\{ \left( x_k^i , y_o^i \right) \mid i = 1,2,\cdots,n; k = 1,2,\cdots,d; o = 1,2,\cdots,l \right\} \quad (5)$$

$$X \in R^{n\times d} \quad Y \in R^{n\times l} \quad (6)$$

After the targeted sample augmentation is performed, it makes the original dataset richer, and here $m$ is defined as the increased number of samples. The new dataset is defined as $D_{new}$ shown in Equation (7). $X$ and $Y$ have also changed as Equation (8).

$$D = \left\{ \left( x_k^i , y_o^i \right) \mid i = 1,2,\cdots,n+m; k = 1,2,\cdots,d; o = 1,2,\cdots,l \right\} \quad (7)$$

$$X \in R^{(n+m)\times d} \quad Y \in R^{(n+m)\times l} \quad (8)$$

### 4.4.2 Custom Model Structures for Patients

This study proposes a form of subtly passing scenario information to the model under the guidance of the above research idea. The operation of this part is shown in Figure 16.

**Adaptive bias adjustment.**

Is there any part of a neural network model design that allows the model to receive specific information directly? The answer is yes. Most ordinary algorithms are one-to-one correspondence between input and output; one input gets one output. There is no connection between different inputs. The structure of the traditional neural network is relatively simple: input layer-hidden layer-output layer.

RNN (David E. Rumelhart et al., 1986) is different from the traditional neural network in that each time, the output of the previous time is brought to the next hidden layer and trained together. Inspired by RNN, this study proposes to take the selected target problem as a particular input and bring it into the hidden layer for operations. The biggest advantage of this approach is that it makes the model more sensitive to the target problem right through the training process. And since only one layer of neural network is added, only one hyperparameter that can be pre-set and one parameter that can be trained, there is little impact on the overall complexity of the model.

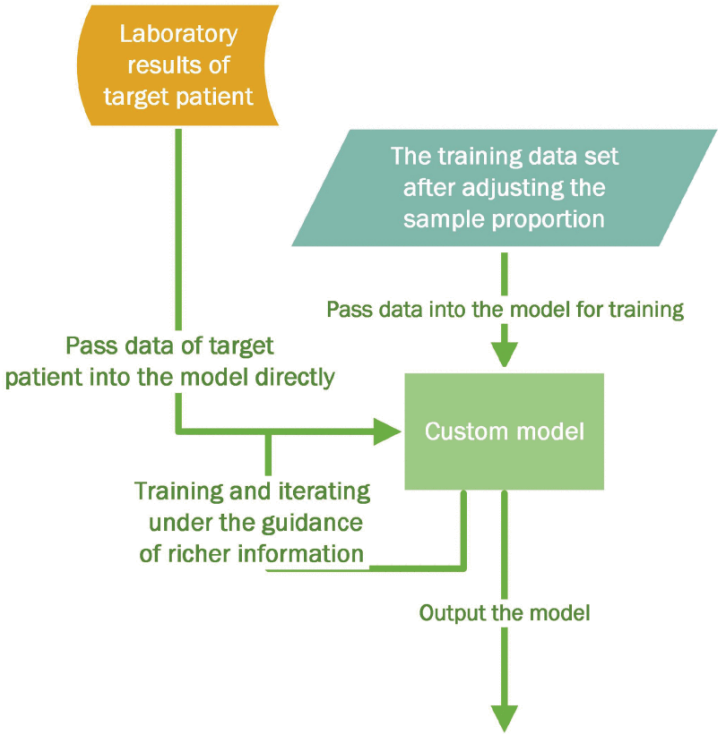



*Figure 16. The framework of subtly passing scenario information to the model*

The specific way is divided into two steps:

After normalizing the data uniformly, the selected target problem is multiplied by a "**bias coefficient:** e" and added to all the input data of the training set. The "**bias coefficient**" can be freely set and represents the initial offset to the target problem on the entire training set. e can be positive or negative, with larger absolute values indicating a greater influence on the training set according to the target problem. The physical meaning of this operation in the sample space can be understood as a shift of all sample points in the sample space in the direction of the selected target problem. If the value of bias coefficient $e = -1$, the origin of the whole sample space coordinate system becomes the selected target problem sample points.

A bias layer with only one parameter is added immediately after the input layer. In the bias layer, the input data are multiplied with the selected target problem by a "**restore coefficient:** -e′" and added again. e′ can be automatically adjusted during the model training by back-propagation. That is the only parameter added to the model that can be automatically adjusted during the training process.

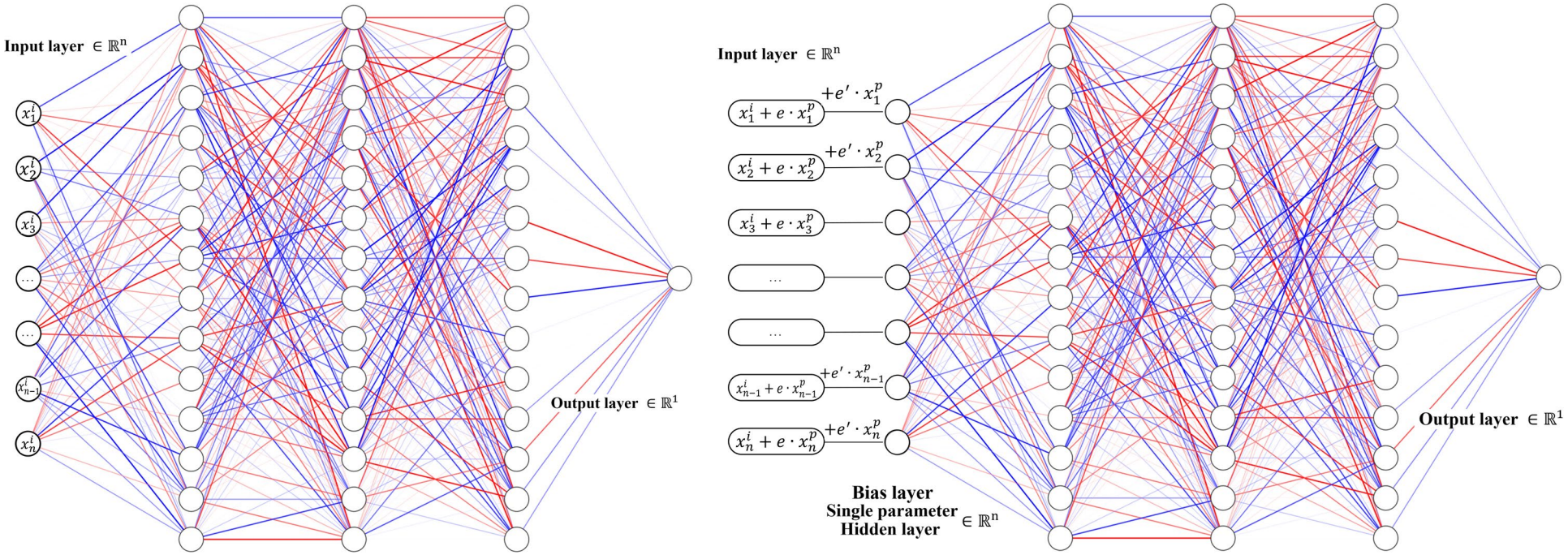



*Figure 17. Structural comparison between the traditional model and custom model.*

Note: $x^i$ is the i-th sample in the training set with total n dimensions. $x^p$ is the target patient sample. $x_k^p$ is a scalar in the kth direction of the vector $x^p$, and it represents a value for a feature of the target patient.

The structural comparison between the traditional model and the custom model is shown in Figure 17. Only one layer is added to the model structure, and only one parameter is added that needs to be trained.

In short, the input data is moved twice bias according to the direction of the selected target problem. The first move is a move of the overall training set according to the predefined parameter $e$. The second move is a move of the samples in the bench during the training process and the training parameter $e'$ by back-propagation at the same time. During this $e'$ iteration, the origin of the coordinate system of the source data set is displaced back and forth in the direction of the selected target problem, which forces the model to be stable for all sample points in the direction of the selected target problem.

At the beginning of this approach design, it is expected that the restore coefficient $e'$ would gradually converge to the opposite of bias coefficient $e$ during the training process, that is $e' = -e$. When $e' = -e$ is achieved, it means that the input passed into the subsequent hidden layer is original data, and all artificially added bias is counteracted.

In the sample space, in addition to the coordinates of the absolute position which contains all the information about the sample, the direction of the sample is also crucial information. In the process of adaptive bias adjustment, the directions of almost all samples change with each change of $e'$, and only the direction of the target sample is always constant. The change of direction vector of each sample in Figure 18 illustrates this change very visually. The left panel represents the unbiased sample space, while the right panel shows the biased sample space. A comparison of the two plots shows that only the direction of the target problem represented by the green square is stable, while the direction of all other samples has changed.

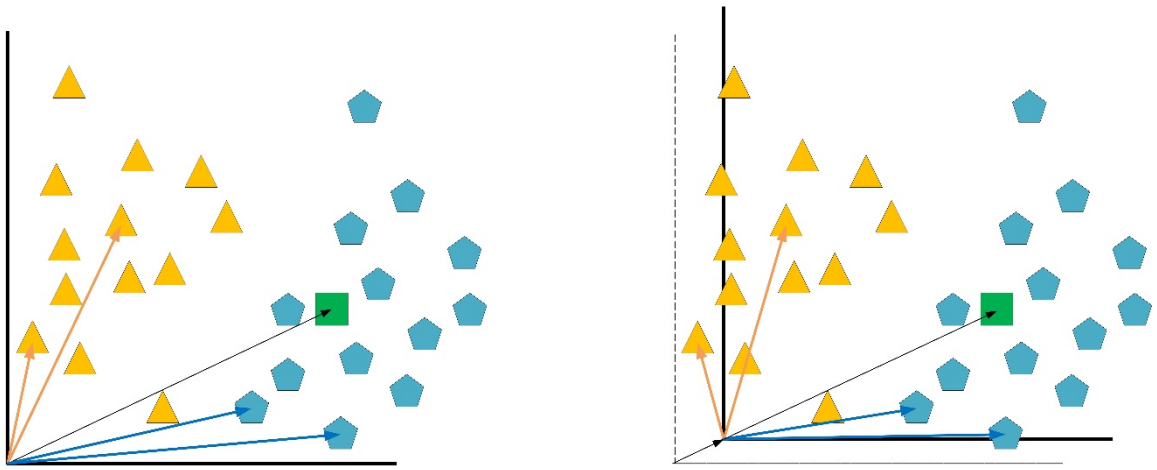


*Figure 18. Adaptive bias adjustment effect comparison chart*

However, during the experiments, it was found that the final result of $e'$ was mostly negative regardless of whether $e$ was set to positive or negative values by reading the final parameter value $e'$ after iteration. In other words, the model tends to orient the overall sample space to the negative half-axis during the learning process. This situation was analyzed: the Rectified Linear Unit (ReLU) (Nair & Hinton, 2010) is used as the activation function used in the subsequent hidden layer, more negative semi-axis variable values are processed to zero, and the sample space is more concentrated, making the overall function more likely to converge. In order not to lose the accuracy and separability of the data in the original sample space, a parameter selection procedure for the $e$ value is subsequently introduced.

The above method can be easily applied to MLP (Multilayer Perceptron). A simplified MLP with only one hidden layer is defined, and its operational logic is summarized in the mathematical formula $f(x)$ shown as equation (7), where $A_o$ and $A_h$ represent the activation function of the activation function of the output layer and the hidden layer, respectively. Typically, **SoftMax** activation functions are used for classification problems, and **Identity** functions are used for regression problems. $W_o$ and $W_h$ represent the weights (also called connection coefficients) of the output layer and the hidden layer, respectively, and $b_o$ and $b_h$ are the biases of the output layer and the hidden layer. The types of $A_o$ and $A_h$ are selected during the model construction phase and can be optimized later as hyperparameters. $W_o$, $W_h$, $b_o$ and

$b_h$ are iteratively updated during the training process.

$$f(x) = A_o\left(b_o + W_o\left(A_h(b_h + W_h X)\right)\right) \quad (7)$$
$$\text{where} \quad W_h \in R^{d\times q} \quad b_h \in R^{1\times q}$$

After introducing the adaptive bias adjustment into the MLP model, the equation changes as shown in Equation (8). $x^q$ is the target problem to be analyzed in the scenario, and $X_q$ is obtained by copying $x^q$ to the same size as X. Among the two newly added variables, $e$ is selected during the model construction phase and can be optimized later as a hyperparameter. $e'$ is updated iteratively during the training process. Only one scalar, $e'$, that needs to be iterated is added during the training process, and the impact on the number of parameters of the model can be negligible.

$$f(x) = A_o\left(b_o + W_o\left(A_h\left(b_h + W_h\left(X + eX_q + e'X_q\right)\right)\right)\right) \quad (8)$$
$$\text{where} \quad W_h \in R^{d\times q} \quad b_h \in R^{1\times q} \quad e \in R^{1\times 1} \quad e' \in R^{1\times 1}$$

Adaptive bias adjustment is not directly applicable to multiple samples for the time being. As an alternative, adaptive bias adjustment can be trained for each sample first, and finally, the effect of customization for the selected target problems can be achieved by model fusion.

### 4.4.3 Validation and Parameter Tuning

Therefore, novel constructs of validation sets are proposed in this study. The operation of this part is shown in Figure 19.

**Novel constructs of validation sets**

When it is necessary to evaluate the excellence of a completed training model, two main criteria are generally used as a reference. One is the loss such as root-mean-square error (RMSE) of the training set and the other is the loss of the validation set. This general case requires us to be able to calculate the loss or RMSE of the validation set, meaning that the correct output of the validation set need to be known. This is possible in the general research and development phase because these validation sets are divided from the complete data set. But how to evaluate the accuracy of the model for the validation set when nobody has the correct output results of the validation set

in the real scenario of the application? This study proposes to find a number of samples from the training set that are closest to the selected target problem as the validation set to evaluate the accuracy and stability of the model for the selected target problem.

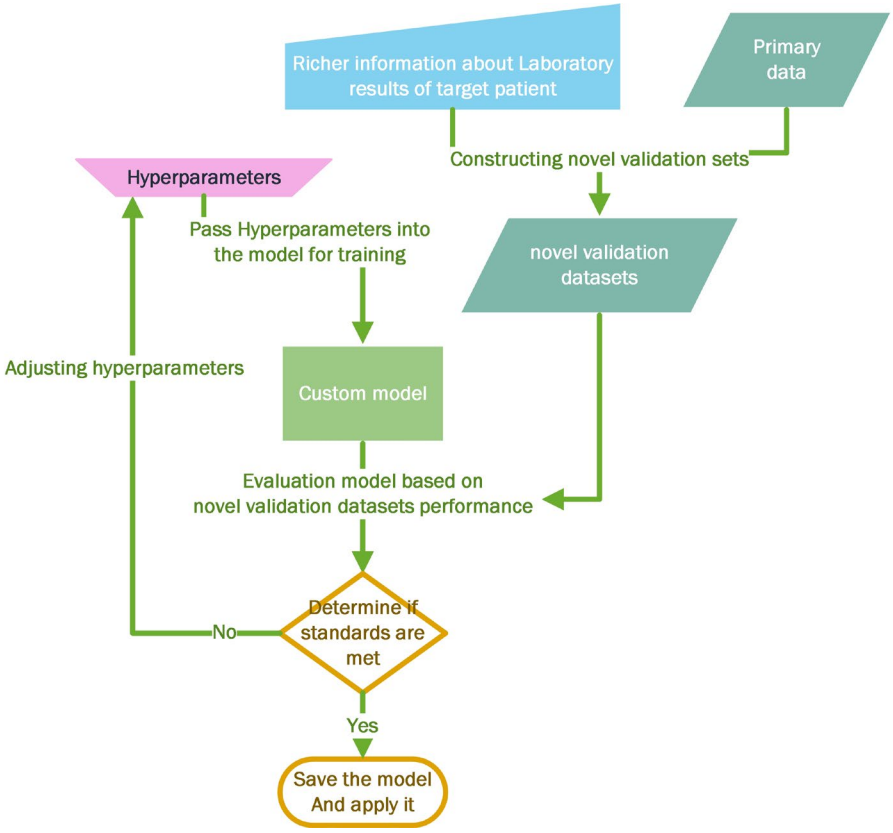



*Figure 19. The framework of Novel constructs of Validation sets*

The result of such an operation mainly affects the operation of the loss function, the original loss function as in Equation (9).

$$J(W_o, W_h, \gamma, \theta, b_o, b_h) = \frac{1}{2}\sum_{i=1}^{n}\sum_{o=1}^{l}\left(y_o'^{i} - y_o^{i}\right)^2 \quad (9)$$

After replacing the new validation set, only the selection of y-values for the loss function formula is changed (as in Equation 10), without adding additional computational effort. The main advantage of this is that it allows the validation set to represent the accuracy and stability of the model for the target problem, rather than the traditional validation set for the entire sample space.

$$J(W_o, W_h, \gamma, \theta, b_o, b_h) = \frac{1}{2}\sum_{i=1}^{n}\sum_{0=1}^{l}\left(y_o'^{i}{}_{new} - y_o^{i}{}_{new}\right)^2 \quad (10)$$

**Optimal parameter selection**

With parameters that evaluate the accuracy and stability of the model with respect to the selected target problem as a guide, Hyperparameter optimization of custom models can be carried out with the help of Optuna (Akiba, Sano, Yanase, Ohta, & Koyama, 2019b) framework. In addition to the usual hyperparameters, such as the number of nodes per layer, epochs, and drop-out ratio, it is found that hyperparametric optimization of the bias coefficient e not only preserves the accuracy and separability of the data in the original sample space as much as possible, but also improves the accuracy of the model for the selected target problem.

**Early termination of training**

In the training process of conventional models, training is usually terminated by setting epochs or terminated early when the validation set loss is no longer decreasing. Since the scheme developed in this thesis has a more explicit selected target problem, the model can be called after each iteration to compute the selected target problem. And the training is terminated early when the output is more stable or the loss in the validation set is no longer significantly reduced.

The entire process is repeated for each patient, as described in Algorithm 1 in appendix.

## 4.5 Experiments

The experiment is divided into two phases: the first phase is the comparison experiment phase, and the second phase is the hyperparameter tuning experiment phase. The comparison experiment phase is to verify the effectiveness of the custom model and compare the performance of the custom model with other commonly used models on some evaluation criteria. The second phase shows the extreme performance level of the custom model by tuning for some hyperparameter settings. The experiments were conducted on the workstation with an Intel Xeon W-2125 CPU, Quadro RTX 4000 with 8 GiB video memory, 32 GiB of DDR4 RAM, and an SSD for secondary storage. All experiments were performed multiple times and the average results were recorded.

### 4.5.1 Parameters of the Approaches

The three main improvement approaches are presented in the methodology phase, all of which introduce some new hyperparameters that were not present during the construction of the original machine learning model. Some of these hyperparameters are presented and analyzed next. In the first phase of the experiments, the parameters of the improvement approaches were chosen using invariant parameter settings to verify the generalizability of the improvement scheme. The following is a description of the special parameters.

**1) Targeted Data Augmentation**

a: Similarity Threshold: By calculating the Mahalanobis distance, the degree of similarity between the samples in the training set and the selected target patient can be obtained, and the smaller the value of the Mahalanobis distance, the more similar it is. A threshold value is set in order to facilitate that samples with a Mahalanobis distance less than the threshold value are identified as extremely similar to the selected target patient, and smote oversampling is performed on these extremely similar samples. In this experiment phase, the similarity threshold was set to a fixed value of 2.5.

b: The Proportion of Minority Classes After Oversampling: The samples identified as extremely similar to the selected target patient were oversampled and expanded. The number of expanded minority classes accounted for the majority of samples (samples considered less similar) up to a set value. In this experiment phase, the proportion of the oversampled minority class was set at a fixed value of 0.3.

**2) Novel Constructs of Validation Set**

The Number of Results Identified as Similar: The samples in the training set are sorted from smallest to largest by calculating the Mahalanobis distance. The number of similar results is set, and the samples that are most similar to the selected target patient are copied from the training set according to the number of similar results to form the validation sets. In this stage, this parameter is set to a fixed number of 10, i.e., the ten samples that are most similar to the selected target patient are selected as the validation set.

**3) Adaptive Bias Adjustment**

Bias Coefficient (e): As introduced in 3.2 above. In this phase, the bias coefficient is set to a fixed value of -0.2.

### 4.5.2 Model Construction

The most basic Back Propagation neural network model (MLP, multilayer perceptron) with three sequential fully connected layers is chosen as the backbone network (Murtagh, 1991). Based on the number of independent variables, the number of nodes in each of the three fully connected layers is set to 120, and each layer is output using the activation function ReLU. The final output layer has only one node and uses sigmoid as the activation function. There are total 30,722 trainable parameters. The Adam (Kingma & Ba, 2014) optimizer, binary_crossentropy, is chosen as the loss function. The overall model construction is simplified as much as possible to evaluate the merit of the final output without using complex techniques. Callbacks are used for the model, val_loss is used as the monitored quantity, and the optimal model is saved. The batch size is chosen to be 256, and the maximum epochs are 100.

### 4.5.3 Comparison Model Selection

After completing the processing of the data, the initial screening of the algorithm was performed with the help of the AutoGluon platform (Erickson et al., 2020). First, the TabularPredictor and TabularDataset classes of AutoGluon are imported, and then the training data are loaded into the AutoGluon TabularDataset object (Mueller, Shi, & Smola, 2020). Next, AutoGluon is used to automatically train different models based on different algorithms, and the trained models are used to evaluate model performance by making predictions on the reserved test set data. And XGBoost and LightGBM are the most two efficient algorithms, so the XGBoost and LightGBM model is chosen as a reference.

XGBoost is a very mature algorithm that can be called directly through the XGBoost interface. The dataset is divided into a training set and a test set in the ratio of 0.2 (15 patients, 108 healthy people need to be distinguished). The model is set as follows:

model_xgboost = XGBClassifier (colsample_bytree = 0.7, learning_rate = 0.03, n_estimators = 100, subsample = 0.7, alpha = 0.9) (Ogunleye & Wang, 2019; Torlay, Perrone-Bertolotti, Thomas, & Baciu, 2017). The results are shown in Table 2.

Table 2. Confusion Matrix of XGBoost Model.

| actual \ predict | Hepatitis = 1 | Hepatitis = 0 |
|---|---|---|
| Hepatitis = 1 | 8 | 7 |
| Hepatitis = 0 | 0 | 108 |

Note: Accuracy = 0.9431, Recall = 0.533, Precision = 1, f1-score = 0.6957

As the confusion matrix demonstrates, the model does not really do a good job. It mainly predicted everything as class 0, so Randomized Search was introduced to try to improve this (Putatunda & Rama, 2018; Linyu Sun, 2020), (Budholiya, Shrivastava, & Sharma, 2022).

The settings for Randomized Search are as follows: params = {'learning_rate': [0.01, 0.05, 0.1,0.2], 'max_depth': [3, 4, 5], 'min_child_weight': [1,3,5,7], 'gamma': [0.0, 0.1, 0.2, 0.3], 'colsample_bytree': [0.3, 0.4, 0.5], 'n_estimators': [750, 1000]}. The new XGBoost model is set as follows: model_xgboost = XGBClassifier (); random_search = RandomizedSearchCV (model_xgboost, param_distributions = params, n_iter = 3, cv = 3, scoring = 'accuracy', n_jobs = -1, verbose = 3). The new results are shown in Table 3, there is indeed some progress.

Table 3. Confusion Matrix of XGBoost Model with Randomized Search.

| actual \ predict | Hepatitis = 1 | Hepatitis = 0 |
|---|---|---|
| Hepatitis = 1 | 10 | 5 |
| Hepatitis = 0 | 0 | 108 |

Note: Accuracy = 0.9593, Recall = 0.6667, Precision = 1.000, f1-Score = 0.8000

Similar to the process of XGBoost optimization, the best results obtained by LightGBM after several hyperparameters optimization are shown in Table 4 (Al Daoud, 2019; Dehua Wang, Zhang, & Zhao, 2017).

Table 4. Confusion Matrix of LightGBM Model After Hyperparameters Optimization.

| actual \ predict | Hepatitis = 1 | Hepatitis = 0 |
|---|---|---|
| Hepatitis = 1 | 10 | 5 |
| Hepatitis = 0 | 2 | 106 |

Note: Accuracy = 0.9431, Recall = 0.6667, Precision = 0.8333, f1-Score = 0.7407

### 4.5.4 Custom Model Performance

#### 1) The Original Performance

Next, it is time for the custom model to make its appearance. In the context of this problem, the laboratory result information is mainly unique to each patient. This session focuses on experimenting with combinations of parameters involved in the three improvement approaches so that the most accurate results can be obtained for each selected target patient. The parameter selection phase has three rounds. In the first round, the number of nodes per layer, epochs, and batch size is determined based on the problem complexity, the number of parameters, and the number of samples. In the second round, repeatable experiments are conducted on a certain number of samples to find parameters that are common to the whole dataset: Similarity threshold, Number of results identified as similar, and Proportion of minority classes after oversampling. These parameters are all closely related to the distribution pattern of the samples in the overall sample space. These parameters are determined as fixed values, which basically satisfy all the selected target patients. In the third round, bias coefficient, and drop-out ratio are then selected according to each selected target patient by the Optuna framework. Optuna framework is actually a repetitive experiment for multiple parameters, and the optimal parameter is output according to the amount of monitoring. The monitored quantity selected is the MAE of the validation set. The variation interval of the bias coefficient is from -0.5 to 0.5, and the variation interval of the drop-out ratio is from 0 to 0.3. The results of the optimal parameters: similarity threshold: 3, Number of results identified as similar: 5, and Proportion of minority classes after oversampling: 0.3. Subsequently added judgment

conditions. 1. Stop targeted data augmentation when there are less than 6 samples below the Similarity threshold. 2. When there are more solutions below the Similarity threshold, the data augmentation selects up to 15 samples as the expansion base.

For the same test set samples as the XGBoost and LightGBM model, each sample is treated as the selected target patient, and the custom model is constructed and classified for each the selected target patient in turn, and the final results are shown in Table 5.

Table 5. Confusion Matrix of Custom Model.

| actual \ predict | Hepatitis = 1 | Hepatitis = 0 |
|---|---|---|
| Hepatitis = 1 | 14 | 1 |
| Hepatitis = 0 | 0 | 108 |

Note: Accuracy = 0.9919, Recall = 0.9333, Precision = 1.000, f1-Score = 0.9655

Table 6. Confusion Matrix of Custom Model on the Entire Dataset.

| actual \ predict | Hepatitis = 1 | Hepatitis = 0 |
|---|---|---|
| Hepatitis = 1 | 49 | 7 |
| Hepatitis = 0 | 1 | 531 |

Note: Accuracy = 0.9864, Recall = 0.8750, Precision = 0.9800, f1-Score = 0.9245

It can be seen that there is a significant improvement over XGBoost and LightGBM, and the entire dataset is iterated in order to better verify the applicability of the method. For the whole dataset, each sample is treated as the selected target patient, and the custom model is constructed and classified for each the selected target patient in turn, and the final results are shown in Table 6.

**2) The Performance with Upgraded Approaches**

By analyzing the results of each selected target patient, the following conclusions are drawn. Although the results are good, it can be still found that: in the real-world environment, the unevenness of the sample space can cause much trouble for the custom model. (1) In the case of insufficient similar samples, if the less similar samples are forcibly selected as the benchmark for augmentation, it will increase the density of the overall

training set in the region that deviates from the selected target patient. It is more sensible to turn off the target sample augmentation at this time. (2) In the case of too many similar samples, the similar sample set will be more evenly distributed in the overall sample space because of its more significant number. Then, the similar sample set no longer has the sensitivity to the selected target patient. At this time, the overall performance of the validation set cannot accurately reflect the accuracy of the custom model for the selected target patient. (3) For some of the selected target patients with a strange distribution, the most similar samples may be of the opposite category. This strange case can not be distinguished by the custom model for the time being, and more comprehensive and rich balanced data are needed to solve this strange case.

The new results are shown in Table 7 after introducing the automatic disablement of the targeted sample augmentation and the setting of the upper limit of similarity samples.

Table 7. Confusion Matrix of Custom Model on the Entire Dataset with Upgraded Approaches.

| predict / actual | Hepatitis = 1 | Hepatitis = 0 |
|---|---|---|
| Hepatitis = 1 | 53 | 3 |
| Hepatitis = 0 | 0 | 532 |

Note: Accuracy = 0.9949, Recall = 0.9464, Precision = 1.000, f1-Score = 0.9725

**3) The Performance for Higher Recall**

Among the target application scenarios of this study, especially when the model is applied to large-scale screening, accuracy is certainly a crucial evaluation criterion. The highest possible accuracy rate allows patients to be accurately identified and treated, and also eliminates the need for additional follow-up testing in healthy individuals.

But the situation changes when hospitals are allowed to diagnose patients who visit them through custom models. For each patient, a false negative poses a much greater risk than a false positive, so it is important to improve the recall rate of the model as much as possible. Guided by such a specific need, the evaluation criteria of the custom model were adjusted. A partial modification of the binary_crossentropy used for the loss function is to

make the model consider that the penalty for false negatives is greater than that for false positives. With such an adjustment, the performance of the model in the test set now is shown in Table 8.

Table 8. Confusion Matrix of Custom Model for Higher Recall.

| actual \ predict | Hepatitis = 1 | Hepatitis = 0 |
|---|---|---|
| Hepatitis = 1 | 15 | 0 |
| Hepatitis = 0 | 9 | 99 |

Note: Accuracy = 0.9268, Recall = 1.000, Precision = 0.625, f1-Score = 0.7692

It can be seen that all patients in this test set were correctly identified, but this led to a more significant decrease in other evaluation criteria. In the recall enhancement experiment on the total data, 55 patients could be identified out of a total of 56 patients.

## 4.6 Comparative Analysis

This study combines target patient analysis into a three-stage process of machine learning data processing, model building, and parameter optimization. The first stage of data processing: Targeted data augmentation is performed on the training data considering the patients' information, so that the dataset generates relevance according to the target patient. By calculating the relevant parameters, such as the Mahalanobis distance, the relevant information within the data is fully explored. The important weight of the samples closely related to the target patient is increased according to scenario requirements. In this process, the target patient information provides the optimization direction for data processing. The second stage is the training model, which uses the target patient information as additional fixed training data to achieve the target patient as a constraint at all times during the training process. The goal of this model is to have better performance in specific target patient, which is different from the goal of previous models that emphasize broad adaptability. In this process, the target patient information provides additional information for model training. The third stage of parameter optimization uses the target patient information as a reference standard. This criterion can both verify the magnitude of the error after each iteration and back-propagate the model for tuning based

on the magnitude of the error, and compare the advantages and disadvantages between several approaches after all training is completed. It provides a reliable reference for parameter tuning related to the target patient, and it is worthwhile to conduct some interesting and meaningful research on them.

Table 9. Richer Comparison of Experimental Results.

| Model | Accuracy | Recall | Precision | F1-score | Author |
|---|---|---|---|---|---|
| **Custom-pro** | **0.9949** | 0.9464 | **1.000** | **0.9725** | Proposed by this work |
| **Custom-recall** | 0.9268 | **1.000** | 0.625 | 0.7692 | Proposed by this work |
| CatBoost | 0.9593 | 0.7333 | 0.9167 | 0.8148 | |
| XGBoost | 0.9593 | 0.6667 | 1.000 | 0.8000 | |
| RFGini | 0.9512 | 0.6667 | 0.9091 | 0.7693 | |
| LightGBM | 0.9431 | 0.6667 | 0.8333 | 0.7407 | |
| Random forests | 0.9187 | 0.6 | 0.6923 | 0.6429 | |
| KNN | 0.8862 | 0.6 | 0.5294 | 0.5625 | |
| AST/ALT ratio | 0.954 | 0.68 | 0.993 | 0.8072 | (Chicco & Jurman, 2021) |
| Fusion model | 0.9545 | 0.8971 | 0.743 | 0.8128 | (Chawathe, 2020) |
| RF and LR | 0.9619 | 0.7153 | 0.9694 | 0.8232 | (T.-H. S. Li, Chiu, & Kuo, 2022) |
| Ensemble model | 0.9559 | | | | (Edeh et al., 2022) |
| Rule-based decision tree | 0.753 | | | | (Lichtinghagen & Hoffmann) |

Note: The custom models at the top of the table are the ones proposed in this chapter, the models in the middle of the table are the results of tuning and optimization using the mature algorithm, and the models at the bottom of the table are the results of other teams using the same dataset. RF is short for Random Forest, LR is short for Linear Regression, DT is short for Decision Tree, and KNN is short for K-NearsNeighbor.

In the testing of the hepatitis C dataset, an extremely accurate model (accuracy of 99.4%) was built without introducing additional information and without having any relevant medical background at all. A comparison of test results among various models is shown in Figure 20. This far exceeds the decision tree model based on expert system logic used in the article by the original provider of the data with a medical background. A richer

comparison of experimental results is detailed in Table 9.

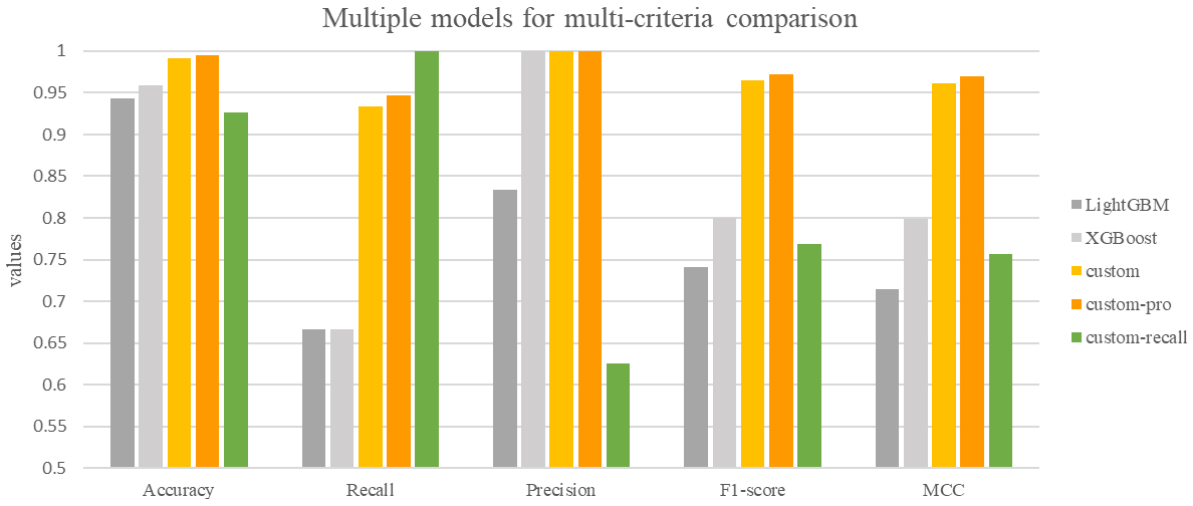



*Figure 20. Comparison of experiments results among various models.*

Note: LightGBM and XGBoost models are the result of parameter optimization. All of the five models compared use the same test set, except for custom-pro, which is the result obtained from the whole dataset. It can be seen that the custom and custom-pro model show advantages in various metrics, and custom-recall shows that the customized solution can achieve almost 100% recall at the expense of some of the remaining criteria.

In testing the hepatitis C dataset, the custom model outperformed the extremely well-developed XGBoost and LightGBM models (selected by AutoGluon). This efficient and accurate model does not require cumbersome tuning and data processing, and does not require medical practitioners to master complex machine learning techniques to use it directly to aid diagnosis.

The analysis time for each individual patient from this part of the case study is about 30s, which can meet the time requirement for medical diagnosis when a patient has finished the blood test. As the dataset expands to the order of magnitude of 10,000, the time to retrain and diagnose for each patient rises to 5 minutes. Such time can be further compressed by upgrading the equipment. The equipment requirements involved in the training and analysis of the model are very common and easy to implement. This means that there is no need for a separate viral test, and that only the simplest of blood tests are

needed to detect the vast majority of patients with hepatitis C, providing a powerful tool for hepatitis C disease control. And this custom model can discard some of the accuracy to achieve higher recall as needed, and the confidence level is greatly improved and no longer relies on the general average level of the model for evaluation, which ensures that the model can be applied to the treatment of specific patients.

## 4.7 Proof of the Principle

In the previous part of this chapter, three specific methods of customizing operations were proposed. Their effectiveness is more clearly explained and demonstrated below.

### 4.7.1 Proof of Targeted Data Augmentation (TDA)

By augmenting the dataset with synthetic samples similar to $x_t$, Targeted Data Augmentation (TDA) effectively increases the representation of the minority class or the underrepresented characteristics in $D$. This augmentation can be seen as adding new points to the feature space that are in the vicinity of $x_t$, thereby enhancing the decision boundary's sensitivity to $x_t$'s characteristics.

**Empirical Risk Minimization Framework**

The standard machine learning model training can be formalized within the Empirical Risk Minimization (ERM) framework (Bassily, Smith, & Thakurta, 2014; Donini, Oneto, Ben-David, Shawe-Taylor, & Pontil, 2018; Rosenberg & Hirschberg, 2007; H. Zhang et al., 2017), where the goal is to find model parameters $\theta$ that minimize the empirical risk:

$$L_{ERM}(\theta; D) = \frac{1}{N}\sum_{i=1}^{N} l(f(x_i; \theta), y_i) \quad (11)$$

Here, $L_{ERM}$ is the empirical loss over the dataset $D$, $l$ is a loss function, $f(x_i; \theta)$ is the prediction of the model parameterized by $\theta$ for the input $x_i$, and $y_i$ is the true label for $x_i$, $N$ is the number of samples in the dataset.

TDA aims to generate synthetic samples $(x_{synth}, y_{synth})$ that are similar to the target data point $x_t$ or the underrepresented class, and add them to the dataset $D$ to form an augmented dataset $D'$.

The new empirical risk with the augmented dataset $D'$ is:

$$L_{ERM}(\theta; D') = \frac{1}{N+M}\left(\sum_{i=1}^{N} l(f(x_i; \theta), y_i) + \sum_{j=1}^{M} l\left(f\left(x_{j,synth}; \theta\right), y_{j,synth}\right)\right) \quad (12)$$

where $M$ is the number of synthetic samples added to the dataset.

To rigorously analyze how Targeted Data Augmentation (TDA) through density estimation and smoothing can enhance the representation of minority classes, an evaluation metric is introduced to validate the effectiveness of TDA. This section will use the concept of Kullback-Leibler (KL) divergence as the evaluation metric to compare the data distributions before and after applying TDA.

**Kullback-Leibler Divergence as Evaluation Metric**

The Kullback-Leibler (KL) divergence (P. Hall, 1987; Hershey & Olsen, 2007; Runnalls, 2007; Van Erven & Harremos, 2014) is a measure of how one probability distribution diverges from a second, expected probability distribution. For discrete probability distributions, $P$ and $Q$ defined on the same probability space, $X$, the KL divergence from $Q$ to $P$ is defined as:

$$D_{KL}(P||Q) = \sum_{x \in \mathcal{X}} P(x) \log\left(\frac{P(x)}{Q(x)}\right) \quad (13)$$

For continuous variables, the sum is replaced by an integral.

Consider a dataset $D = \{(x_i, y_i)\}_{i=1}^{N}$ with $x_i \in R^d$ and $y_i \in \{0,1\}$. Assume the empirical data distribution for the dataset is $P$, and after applying TDA, we obtain a new distribution $P'$. Mathematically, the modification can be seen as:

$$P'(x) = (1 - \alpha)P(x) + \alpha \Delta(x) \quad (14)$$

where $\Delta(x)$ represents the distribution of synthetic samples added near the target data point(s), and $0 < \alpha < 1$ is a blending parameter indicating the proportion of synthetic data. Since $\Delta(x)$ represents the distribution of the set produced according to the case of the target variable $x_t$, that:

$$\sum_{x \in X} \Delta(x) \log\left(\frac{\Delta(x)}{Q(x)}\right) < \sum_{x \in X} P(x) \log\left(\frac{P(x)}{Q(x)}\right) \quad (15)$$

The goal is to demonstrate that $P'$ is a better representation of the $x_t$ compared to $P$.

To prove this, we aim to show that $\mathrm{P}'$ is closer to the ideal distribution $\mathrm{Q}$ of the $\mathrm{x_t}$ than $\mathrm{P}$ is, using KL divergence as the measure of closeness. We need to demonstrate that:

$$D_{\mathrm{KL}}(P'||Q) < D_{\mathrm{KL}}(P||Q) \tag{16}$$

implying $\mathrm{P}'$ is closer to the ideal distribution $\mathrm{Q}$ than $\mathrm{P}$ is.

The KL divergence from $\mathrm{P}'$ to $\mathrm{Q}$ is:

$$D_{\mathrm{KL}}(P'||Q) = \sum_{x\in\mathcal{X}}((1-\alpha)P(x)+\alpha\Delta(x))\log\left(\frac{(1-\alpha)P(x)+\alpha\Delta(x)}{Q(x)}\right) \tag{17}$$

So:

$$D_{\mathrm{KL}}(P||Q) - D_{\mathrm{KL}}(P'||Q) = \sum_{x\in\mathcal{X}} P(x)\log\left(\frac{P(x)}{Q(x)}\right) - \sum_{x\in\mathcal{X}}((1-\alpha)P(x)+\alpha\Delta(x))\log\left(\frac{(1-\alpha)P(x)+\alpha\Delta(x)}{Q(x)}\right) \tag{18}$$

Simplification and Utilization of Logarithmic Properties:

$$\begin{aligned}
\mathrm{T} &= \sum_{\mathrm{x}\in\mathrm{X}}\left[\mathrm{P(x)}\log\left(\frac{\mathrm{P(x)}}{\mathrm{Q(x)}}\right) - \left((1-\alpha)\mathrm{P(x)}+\alpha\,\Delta\,(\mathrm{x})\right)\log\left(\frac{(1-\alpha)\mathrm{P(x)}+\alpha\,\Delta\,(\mathrm{x})}{\mathrm{Q(x)}}\right)\right] \\
&= \sum_{\mathrm{x}\in\mathrm{X}}\Big[\mathrm{P(x)}\big[\log\big(\mathrm{P(x)}\big) - \log\big(\mathrm{Q(x)}\big)\big] \\
&\qquad - \left((1-\alpha)\mathrm{P(x)}+\alpha\,\Delta\,(\mathrm{x})\right)\Big[\log\left((1-\alpha)\mathrm{P(x)}+\alpha\,\Delta\,(\mathrm{x})\right) - \log\big(\mathrm{Q(x)}\big)\Big]\Big] \\
&= \sum_{\mathrm{x}\in\mathrm{X}}\Big[\mathrm{P(x)}\log\big(\mathrm{P(x)}\big) - \left(\alpha\,\Delta\,(\mathrm{x}) - \alpha\mathrm{P(x)}\right)\log\big(\mathrm{Q(x)}\big) \\
&\qquad - \left((1-\alpha)\mathrm{P(x)}+\alpha\,\Delta\,(\mathrm{x})\right)\log\left((1-\alpha)\mathrm{P(x)}+\alpha\,\Delta\,(\mathrm{x})\right)\Big]
\end{aligned} \tag{19}$$

Given that the logarithm function is concave, and $(1-\alpha)+\alpha = 1$, we can apply Jensen's inequality (Dragomir, 2013; Hansen & Pedersen, 2003) for the expectation of a concave function,

$$\begin{aligned}
\mathrm{T} > \sum_{\mathrm{x}\in\mathrm{X}}\Big[&\Delta\,(\mathrm{x})\log\left(\Delta\,(\mathrm{x})\right) - \Delta\,(\mathrm{x})\log\big(\mathrm{Q(x)}\big) + \mathrm{P(x)}\log\big(\mathrm{Q(x)}\big) \\
&- \left(\alpha\,\Delta\,(\mathrm{x}) - \alpha\mathrm{P(x)}\right)\log\big(\mathrm{Q(x)}\big) \\
&- \left((1-\alpha)\mathrm{P(x)}+\alpha\,\Delta\,(\mathrm{x})\right)\log\left((1-\alpha)\mathrm{P(x)}+\alpha\,\Delta\,(\mathrm{x})\right)\Big]
\end{aligned}$$

$$= \sum_{x \in X} \Big[ \Delta(x) \log\Big(\Delta(x)\Big) + (1+\alpha)(P(x) - \Delta(x)) \log\big(Q(x)\big) - \Big((1-\alpha)P(x) + \alpha\Delta(x)\Big) \log\Big((1-\alpha)P(x) + \alpha\Delta(x)\Big)\Big] \geq 0 \tag{20}$$

Concluding $T(x) > 0$

Upon cancellation and simplification, the dominance of positive contributions illustrates $T(x) > 0$. This analysis hinges on the critical role of $\alpha$ and the strategic design of $\Delta(x)$ in TDA to enhance the representation of minority classes. The proof fundamentally rests on the properties of the logarithmic function, the strategic composition of $\Delta(x)$, and the mathematical leverage provided by Jensen's inequality.

This rigorous simplification underscores the effectiveness of TDA in reducing the KL divergence between the modified distribution $P'$ and the ideal distribution $Q$, thereby mathematically validating the beneficial impact of TDA on enhancing model performance for minority classes or characteristics.

To dive deeper into the effects of Targeted Data Augmentation (TDA) on gradient shifting and the loss landscape, next part start by formalizing the notion of the loss function's gradient and how TDA affects this gradient. The ultimate goal is to demonstrate mathematically that TDA encourages the model to discover parameter settings $\theta$ that are more discriminative for minority classes.

The gradient of the original loss function (Barron, 2019; Christoffersen & Jacobs, 2004; Q. Wang, Ma, Zhao, & Tian, 2020) with respect to the model parameters $\theta$ is:

$$\nabla_\theta L_{original}(\theta; D) = \frac{1}{N} \sum_{i=1}^{N} \nabla_\theta l(f(x_i; \theta), y_i) \tag{21}$$

After augmentation, the gradient of the loss function becomes:

$$\nabla_\theta L_{augmented}(\theta; D') = \frac{1}{N+M} \left( \sum_{i=1}^{N} \nabla_\theta l(f(x_i; \theta), y_i) + \sum_{j=1}^{M} \nabla_\theta l\big(f\big(x_{j,synth}; \theta\big), y_{j,synth}\big) \right) \tag{22}$$

Given the synthetic samples are similar to the minority class (which is similar to $x_t$), TDA introduce new gradients $\nabla_\theta l\big(f\big(x_{j,synth}; \theta\big), y_{j,synth}\big)$ which are theoretically aligned with the minority class learning direction but with potentially higher magnitude due to targeted augmentation. Therefore, the sum of gradients after TDA contains an amplified minority

class signal.

Simplifying further, the gradients from synthetic samples are considered to have a scalar multiple $k > 1$ of the magnitude of average gradients from original minority class samples, reflecting the targeted amplification. The contribution of synthetic samples to the gradient vector can be seen as:

$k \cdot \frac{1}{N_{min}} \sum_{min} \nabla_\theta l(f(x_i; \theta), y_i)$ where $N_{min}$ is the number of original minority class samples, and the sum is over these $N_{min}$ samples.

The augmented gradient vector can be rewritten as:

$$\nabla_\theta L_{augmented}(\theta; D') = \frac{1}{N+M}\left(N \cdot \overrightarrow{G_{original}} + kM \cdot \frac{1}{N_{min}} \sum_{min} \nabla_\theta l(f(x_i; \theta), y_i)\right) \quad (23)$$

Given $k > 1$ and the additional synthetic gradients are aligned with the minority class signal, the second term effectively increases the overall magnitude of the gradient vector related to minority class learning.

This is because the augmentation not only adds to the existing signal but introduces an amplified component related to the minority class, thereby increasing the total gradient vector's magnitude. This amplified component makes the model more sensitive to the minority class nuances, effectively enhancing its discriminative power.

### 4.7.2 Proof of Adaptive Bias Adjustment (ABA)

Adaptive Bias Adjustment (ABA) introduces an additional step in this process by first altering the input data $x$ using a bias coefficient $e$ related to the target patient's data $x_q$ and then adjusting this bias within the model itself using a restore coefficient $e'$. Mathematically, this can be described as follows:

Initial Bias Adjustment:

$$x_{ajse} = x + e \cdot x_q \quad (24)$$

To counterbalance or adjust this initial bias during model training, this chapter introduces a restore coefficient $e'$, leading to an adaptive bias adjustment in the input features as follows:

$$x_{aatv} = x_{ajse} + e' \cdot x_q = x + (e + e') \cdot x_q \quad (25)$$

where $x_{ajse}$ represents the adjusted input features, and $e$ is the bias coefficient that is predetermined before training. So, the Model Prediction Function with Adaptive Bias:

$$f(x_{ajse}) = A\left(b_o + W_o \cdot A\left(b_h + W_h \cdot \left(x_{ajse} + e' \cdot x_q\right)\right)\right) \quad (26)$$

where: $A$ represents the activation function applied at each layer, $W_o$ and $W_h$ are the weights of the output and hidden layers, respectively, $b_o$ and $b_h$ are the biases of the output and hidden layers, respectively, $e'$ is the restore coefficient learned during training to adjust the initial bias introduced by $e$.

The objective during training is to find the optimal set of parameters ($W$, $b$, and $e'$) that minimizes the loss function $L$, which measures the difference between the model's predictions and the actual target values. The loss function could be, for example, the mean squared error (MSE) for regression tasks:

$$L(W, b, e') = \frac{1}{N}\sum_{i=1}^{N}\left(y_i - f(x_{i,ajse})\right)^2 \quad (27)$$

where $N$ is the number of training samples.

The mathematical justification for the effectiveness of Adaptive Bias Adjustment lies in its capacity to explicitly model and adjust for the peculiarities of the target patient's data within the learning process. By incorporating $x_q$ directly into the input features and allowing the model to learn an optimal $e'$ to adjust this bias, the model becomes more attuned to the characteristics of the target patient, thereby improving its predictive performance for this specific individual.

To understand why this approach enhances the model's sensitivity to the target, consider the gradient of the loss function with respect to the model's weights ($W$) during training. The gradient indicates the direction in which the model's parameters should be adjusted to minimize the loss. With the inclusion of $e \cdot x_q$, the gradient becomes sensitive not just to the differences between the model's predictions and actual target values but also to how these differences relate to the target patient's characteristics.

For a simple model, the gradient of the loss $L$ with respect to weights $W$ can be expressed as (Gao, Gouk, Yang, & Hospedales, 2022; L. Li, Doroslovački, & Loew, 2020; Ribeiro & Elsayed, 1995):

$$\nabla_W L = -\frac{2}{N}\sum_{i=1}^{N}\left(y_i - f\left(x_{i,ajse}\right)\right)\cdot\frac{\partial f}{\partial W} \tag{28}$$

where: $f\left(x_{i,ajse}\right)$ is the model's prediction function applied to the adjusted input features, $y_i$ is the actual target output for the $i$th training sample.

Given that $x_{ajse}$ includes $e\cdot x_q$, the derivative $\frac{\partial f}{\partial W}$ and hence the gradient $\nabla_W L$ encapsulates information regarding how adjustments to $W$ impact the loss in the context of the target patient's specific data.

The direct inclusion method ensures that the loss minimization process—and consequently, the model updates—are performed in a way that is inherently tied to the target patient's characteristics. This leads to a model whose parameters are optimized not just for general accuracy across all samples but are finely tuned to enhance prediction accuracy for the target patient.

Then, $f$ is considered as a function that processes $x_{i,aatv}$ as a whole, before $f$ was a function that processed $x_{i,ajse}$. The training objective is to minimize the loss function L, which could be expressed as the mean squared error (MSE) for a regression task:

$$L(W,b,e') = \frac{1}{N}\sum_{i=1}^{N}\left(y_i - f\left(x_{i,aatv}\right)\right)^2 \tag{29}$$

To find the optimal $e'$ alongside $W$ and $b$, gradient descent is employed. The gradient of the loss function with respect to $e'$ is:

$$\frac{\partial L}{\partial e'} = \frac{2}{N}\sum_{i=1}^{N}\left(f\left(x_{i,aatv}\right) - y_i\right)\cdot\frac{\partial f\left(x_{i,aatv}\right)}{\partial e'} \tag{30}$$

Given that $x_{aatv} = x + (e + e')\cdot x_q$, the derivative of $f$ with respect to $e'$ can be expressed via the chain rule as:

$$\frac{\partial f\left(x_{i,aatv}\right)}{\partial e'} = \frac{\partial f}{\partial x_{i,aatv}}\cdot\frac{\partial x_{i,aatv}}{\partial e'} = \frac{\partial f}{\partial x_{i,aatv}}\cdot x_q \tag{31}$$

Hence, updating $e'$ during each iteration of gradient descent involves:

$$e' \leftarrow e' - \alpha\cdot\frac{\partial L}{\partial e'} \tag{32}$$

where $\alpha$ is the learning rate.

The optimization process iteratively adjusts $e'$ to find an optimal balance between the initial bias introduced by $e$ and the model's need to accurately predict outcomes for the

target patient. As $e'$ converges to an optimal value, the model becomes more finely tuned to the characteristics specific to $x_q$, enhancing its prediction accuracy for this individual.

The adaptive bias adjustment ensures that the model's predictions are not merely based on generalized patterns learned from the training data but are also influenced by the specific data characteristics of the target patient. This method effectively incorporates the uniqueness of $x_q$ into the model, allowing for personalized predictions. The optimization of $e'$ ensures that the model does not overly adjust its predictions based on the initial bias, maintaining a balance between generalizability and personalization.

### 4.7.3 Proof of Novel Constructs of Validation Set (NCV)

The Novel Constructs of Validation Set (NCV) proposes selecting the validation set $V$ such that:

$$V = \{(x\_j, y\_j) \mid d(x\_j, x\_t) \leq \theta, j = 1, 2, \ldots, m\} \quad (33)$$

where $d(x_j, x_t)$ represents a distance metric between the sample $x_j$ and the target sample $x_t$, and $\theta$ is a threshold defining "closeness" to $x_t$. The set $V$ thus includes $m$ samples that are closest to $x_t$ according to the distance metric $d$.

By selecting samples close to $x_t$, $V$ becomes more representative of the data distribution around the target sample. This is particularly important in personalized models, where the model's ability to accurately predict for $x_t$ is paramount. The representativeness of $V$ ensures that the validation metrics (accuracy, precision, recall, etc.) are more indicative of the model's performance in the specific context of $x_t$.

To rigorously prove that the use of a validation set $V$ constructed from samples closest to the target sample $x_t$ ensures that the model tuning process is more aligned with the target sample's specific characteristics, an evaluation metric is introduced and then the impact on this metric is analyzed of using $V$.

The MSE (Mean Squared Error) for a set of predictions $\hat{y}_i$ against the true values $y_i$ is defined as:

$$\text{MSE} = \frac{1}{m}\sum_{i=1}^{m}(\hat{y}_i - y_i)^2 \quad (34)$$

where $m$ is the number of samples in the validation set $V$, $\hat{y}_i$ is the predicted value for the i-th sample, and $y_i$ is the corresponding true value.

Before the introduction of the measure, a generic validation set $V_{generic}$ is introduced which is composed of randomly selected samples from the dataset. The MSE computed using $V_{generic}$ reflects the model's performance across a broad spectrum of the data distribution, potentially diluting the focus on the target sample's specific characteristics.

$$MSE_{generic} = \frac{1}{m}\sum_{i=1}^{m}(\hat{y}_i - y_i)^2 \tag{35}$$

After the introduction of $V$, constructed specifically around $x_t$, the MSE reflects the model's performance on samples that are similar to $x_t$, emphasizing the error in the context most relevant to $x_t$.

$$MSE_V = \frac{1}{m}\sum_{i=1}^{m}\left(\widehat{y_{V_i}} - y_{V_i}\right)^2 \tag{36}$$

where $\widehat{y_{V_i}}$ and $y_{V_i}$ are the predicted and true values, respectively, for samples in $V$.

To formalize the argument, let $\theta$ represent the model hyperparameters. The tuning process seeks to find $\theta^*$ that minimizes $MSE_V$:

$$\theta^* = \arg\min_{\theta}\frac{1}{m}\sum_{i=1}^{m}\left(\widehat{y_{V_i}}(\theta) - y_{V_i}\right)^2 \tag{37}$$

This optimization process inherently aligns $\theta^*$ with the characteristics of the target sample $x_t$, as it minimizes error specifically for $V$, a set of samples sharing characteristic of $x_t$, making $V$ a highly representative sample set for tuning the model to $x_t$ 's specific scenario. By optimizing $\theta$ to minimize $MSE_V$, the model explicitly focuses on reducing errors for samples that resemble $x_t$, thus ensuring that $\widehat{y_{V_i}}(\theta)$ closely matches $y_{V_i}$ for all $i$ in $V$.

To further refine and mathematically substantiate the principle that targeted selection of validation sets (V) reduces variance in model evaluation, we should first introduce an evaluation metric that can quantitatively measure the variance in model performance metrics across different validation sets. One common approach to evaluating model stability is to use the variance of the model's performance metric (such as accuracy, precision, or recall) across multiple iterations of training and validation cycles. For the purpose of this analysis, the variance of accuracy is used as the primary evaluation metric.

The accuracy of the model on a validation set $V$ is defined as $A(V)$, which is the proportion of correctly predicted samples out of all samples in $V$. For a series of $k$ different validation sets $V_1, V_2, \ldots, V_k$, the variance of accuracy across these sets is given by:

$$\sigma_A^2 = \frac{1}{k-1}\sum_{i=1}^{k}(A(V_i) - \overline{A})^2 \tag{38}$$

where $\overline{A}$ is the mean accuracy across all $k$ validation sets:

$$\overline{A} = \frac{1}{k}\sum_{i=1}^{k} A(V_i) \tag{39}$$

In traditional random selection, each validation set $V_i$ is likely to have a varied representation of the data distribution, especially in personalized settings where the target sample $x_t$ has specific characteristics not uniformly distributed across the dataset. This variability in representation can lead to higher fluctuations in $A(V_i)$ values across iterations, resulting in a higher $\sigma_A^2$.

With the targeted selection, each $V_i$ is constructed to closely mirror the data distribution around the target sample $x_t$, ensuring each validation set is more consistent with $x_t$'s specific context. This consistency leads to less fluctuation in $A(V_i)$ values across iterations, aiming for a lower $\sigma_A^2$.

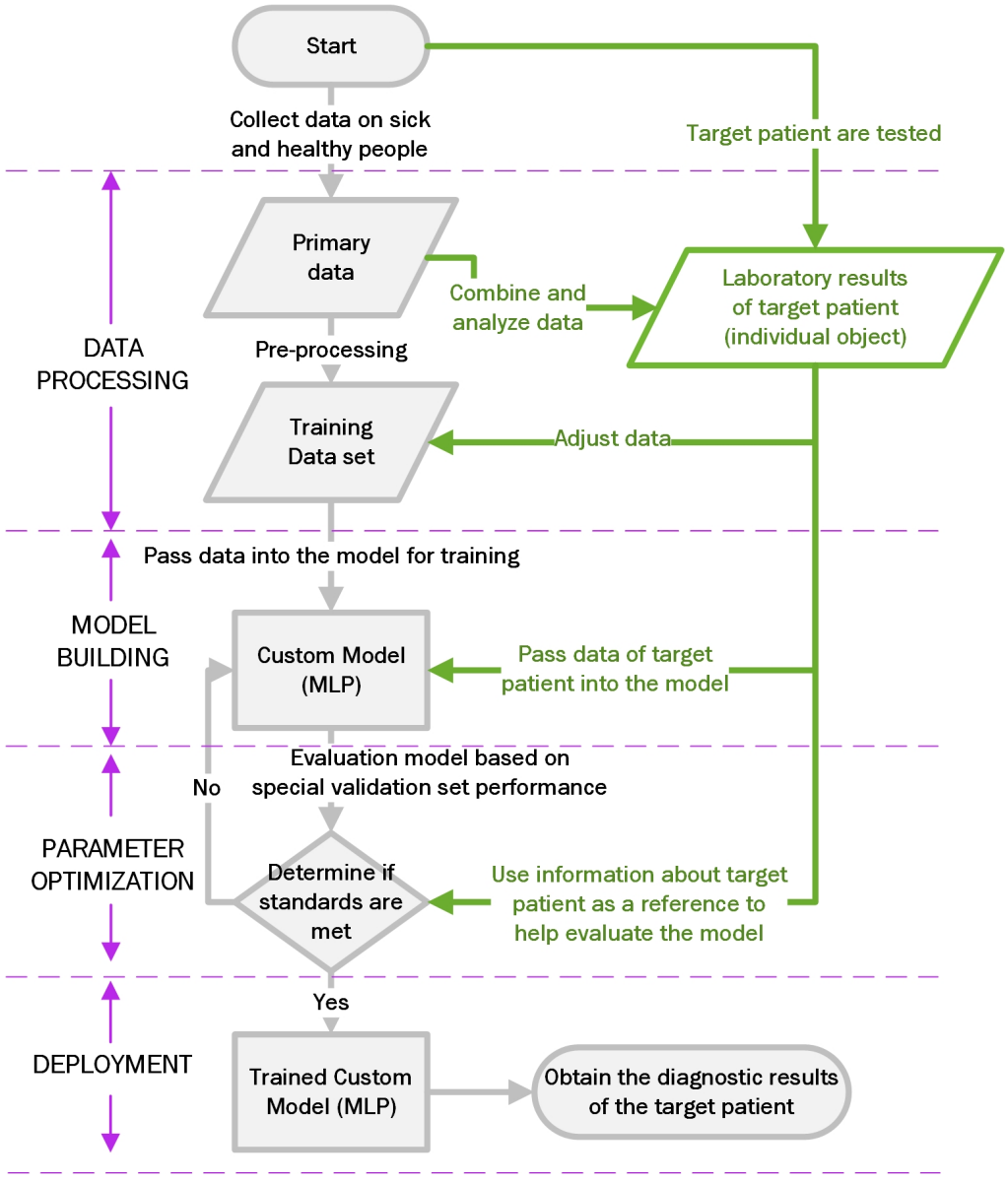
## 4.8 Summary

In this chapter, the development and application of machine learning models tailored to single individual objects have been meticulously explored, particularly within the context of diagnosing Hepatitis C. This personalized approach represents a pivotal shift from conventional, generalized models to the ones that are intricately designed around the unique data profiles of individual subjects. Next part delves deeper into the significance of this approach and its broader implications for precision medicine.

**Innovations and Contributions**

The research has underscored the imperative of personalizing machine learning algorithms to accommodate the inherent complexity and dynamism of individual health profiles. By implementing strategies such as targeted data augmentation and adaptive bias

adjustment, this chapter has transcended conventional model limitations, ensuring that the models are finely attuned to the subtle variances in physiological and environmental factors unique to each patient. This degree of customization in machine learning applications within healthcare is unparalleled and signifies a pivotal advancement toward achieving




personalized diagnostics and treatment plans. The solution proposed in this chapter to provide a custom model for each patient is shown in Figure 21. The grey parts are what the traditional solution contains and the green parts are the approaches proposed in this study.

*Figure 21. Flowchart of customised solutions for each individual object.*

**Addressing Core Challenges**

The bespoke models developed herein address critical challenges traditionally faced by machine learning in healthcare diagnostics, including data imbalance, insufficient accuracy, interpretability issues, and the need for adaptability in dynamic health environments.

Addressing Data Imbalance and Accuracy. Through the deployment of targeted data augmentation, this study significantly mitigated the pervasive issue of data imbalance, which traditionally skewed model predictions toward majority classes. By enhancing the representativeness of minority classes closely aligned with the individual's data profile, the models showcased heightened sensitivity and specificity in diagnostics, thereby elevating both accuracy and efficiency. This bespoke approach also circumvented the generalization pitfalls of conventional models, ensuring a nuanced grasp of individual physiological variances and their implications on disease progression.

Enhancing Model Interpretability. The customization of models inherently fosters greater interpretability and transparency. By simplifying model structures around the unique data signature of an individual and employing techniques like adaptive bias adjustment, this research has illuminated the decision-making pathways of machine learning diagnostics. Such clarity in model operations not only bolstered trust among medical practitioners and patients but also paved the way for more informed and personalized treatment decisions.

Navigating Dynamic Environments. The personalization of machine learning models inherently accommodated the dynamism of individual health states over time. By integrating strategies for dynamic learning and model adaptability, the research presented herein offers a robust framework for models to evolve in concert with changes in individual health indicators. This adaptability assured sustained model relevance and accuracy, a critical advantage over static traditional models.

These approaches not only enhance model sensitivity and specificity but also provide a framework for models to evolve in synchronization with changes in a patient's health state, thereby maintaining continuous relevance and accuracy.

**Future Directions**

Looking ahead, this research paves the way for expansive exploration into the applicability of personalized machine learning models across a spectrum of diseases, the integration of multimodal data sources, and the enhancement of real-time model adaptability. However, this journey is accompanied by challenges that necessitate further inquiry, including scalability, broader disease applicability, and the ethical ramifications of personalized data usage. It is imperative that the ongoing advancement of these models is steered by stringent ethical standards to adeptly navigate the intersection of innovation and patient privacy.

In conclusion, the evolution of machine learning models tailored to individual subjects stands as a cornerstone in the quest for personalized medicine. This chapter lays a solid foundation for future where diagnostic models transcend their role as mere analytical tools, becoming integral partners in delivering care that is truly personalized. As we forge ahead in refining these models, the vision of individualized healthcare, attuned to the unique needs of each patient, inches ever closer to reality.

*Transition Paragraph: Chapter four approaches scenario-based machine learning by focusing on individual objects, amplifying the importance of individuals as much as possible. This intense concentration on individual requirements logically leads to the successful implementation of custom models. However, focusing inevitably leads to overlooking broader aspects as attention to specific details can cause one to miss surrounding information. Therefore, in the following chapter, we will discuss implementing scenario-based machine learning from a broader perspective, considering environmental information and scenario demands to enrich our understanding and application.*

# CHAPTER 5 MACHINE LEARNING MODELS BASED ON THE SPECIFIC REQUIREMENTS OF THE APPLICATION SCENARIO

## 5.1 Introduction

In the rapidly evolving field of machine learning, the pursuit of generalizable models has often overshadowed the nuanced needs of specific application scenarios. This chapter addresses the gap by focusing on the development of bespoke machine learning models tailored to meet the unique demands of particular operational contexts. Unlike conventional models, which are designed to handle a broad spectrum of data types and scenarios, these specialized models prioritize the intricate characteristics and requirements of their targeted environments. This section discusses the scope of traditional machine learning that is difficult to cover, as well as some conceptual original rational analyzes of machine learning models based on specific requirements of the application scenario.

### 5.1.1 Problem Analysis

While individual information is undoubtedly important, without the context of environmental factors, it becomes as insubstantial as a tree without roots or water without a source (Filipe, Ruivo, & Oliveira; Kurebayashi, Komuro, & Hirai; Sarker, Kayes, & Watters; Stetter et al.; Virani, Ji-Woong, Phoha, & Ray). The scene contains a plethora of information that, although not directly related to the subject under analysis, can influence it. If this contextual information is not properly considered, the conclusions drawn will inevitably be biased (Bellamy et al.; Gianfrancesco, Tamang, Yazdany, & Schmajuk; N. N, P, C, & D; P, Petko, & R; van Giffen, Herhausen, & Fahse). Moreover, different application scenarios represent different target requirements. Achieving a proper balance between objectives and resources within a specific context is an art of elegance. In addition to the limitations mentioned in the previous chapter, the current field of machine learning faces further deficiencies that hinder the real-world application of machine learning models in specific scenarios.

**Limitations of General Models.** Current machine learning models often aim for high

generalizability, designed to handle a broad range of data types and application scenarios (D. A. A et al.; Chattopadhyay, Balaji, & Hoffman, 2020; Ishaan & David; H. S. Yang, Pan, et al.). However, this strategy of pursuing universality often sacrifices the deep mining and utilization of specific domain data characteristics, leading to relative deficiencies in performance and accuracy in specific application environments. This phenomenon stems from the model's inability to fully adapt to the unique data distribution and inherent patterns of a specific scenario, thus limiting its effectiveness. This challenge highlights the importance of customizing algorithms and models for specific application scenarios to ensure that models can deeply understand and utilize the unique characteristics of specific domain data.

**Low Resource Efficiency.** Many advanced machine learning algorithms, especially deep learning models, demand substantial computational resources, which becomes a significant barrier in environments with limited computing capabilities (Alberto et al.; Chunlei et al.; "Deep Learning on Edge," ; Hamid, Ajay, E, & Bahram; Mi et al.; Taye & Yehualashet). This is particularly critical in resource-constrained environments such as edge devices and mobile platforms. The issue arises from the models' requirement for extensive data processing and complex computations during training and inference phases, making these models challenging to deploy in edge computing devices or resource-limited application scenarios (Attila, Gábor, & R; Cybenko G; Jonatan, M, O, V, & Nguyen; C. T. Neil, K, Keeheon, & Gabriel; Nicholas & Vadim; Omar et al.; A. Robert, Saketh, Brandon, Gu-Yeon, & D). Achieving a balance between efficiency and accuracy in the specific requirements of a given scenario is a difficulty. When considering the needs of the scenario, the original problem transforms into a typical multi-objective optimization problem, where not only the accuracy of detection (such as sensitivity and specificity) must be considered but also multiple dimensions including cost, speed, and usability. Furthermore, when dealing with different types of diseases, the problem becomes even more complex, as different diseases may require different detection strategies and optimization metrics.

**Data privacy and security challenges.** With the surge in data volume and the widespread deployment of machine learning applications, issues of data privacy and security have become increasingly significant. Existing machine learning frameworks and

algorithms often lack built-in privacy protection and security mechanisms at the design stage, leading to potential data breaches and security risks (Boenisch, Battis, Buchmann, & Poikela; K. G. D; Duddu, Szyller, & Asokan; Hideaki; Hintersdorf, Struppek, & Kersting; Nicolas; Nicolas, P, Arunesh, & Michael; Papernot, McDaniel, Sinha, & Wellman). This issue partly originates from the challenges associated with integrating data privacy protection technologies (such as differential privacy and homomorphic encryption), and the performance overhead these technologies may introduce (Anmar, Sufyan, & Belal; Arnaud, Marina, Oana, Renaud, & Cédric; Prateek; Rezak, S, S, & Thinh; P. Robert, Daniel, & Peizhao; P. Robert, Daniel, Peizhao, M, & Zhipeng). The development and deployment of machine learning models must take these factors into account.

**Insufficient interdisciplinary integration.** Despite the theoretical potential of machine learning technologies for cross-domain applications, in practice, the integration between technology and domain knowledge is often limited. This challenge arises from the barriers of knowledge and language between different disciplines, as well as the lack of effective interdisciplinary collaboration frameworks and mechanisms, limiting the potential of machine learning technologies to address complex, cross-domain problems (Aryal et al.; Grichi, Eghan, & Adams; Littmann et al.; S. Park). In specific application scenarios, an extensive body of mature knowledge or regulations often exists. For machine learning models to excel in such scenarios, they must adhere to relevant guidance. Yet, existing algorithms rarely accommodate this aspect (Christopher & N; Himel & Victor; Lucia; Sagar, Deepali, & V; Tim, S, Julian, & Bernd; Ting; Ting, S, & T).

**Limitations in innovation and theoretical development.** An over-reliance on general models and traditional algorithms can stifle theoretical innovation and technological progress within the machine learning field (Barham & Isard; Belkin, Hsu, Ma, & Mandal; Pearl). This phenomenon is partly due to research resources and attention being focused on optimizing existing technologies rather than exploring new model architectures or algorithms, neglecting the exploration of new theoretical questions and solutions. To drive continuous progress in the field of machine learning, we must move beyond dependence on existing models and algorithms and explore new theoretical frameworks and computational paradigms. This includes seeking inspiration from

fundamental mathematics and statistical theories, as well as exploring novel computational models that better simulate the human brain's information processing methods (Helmstaedter; W. Jiang; Marblestone, Wayne, & Kording; Rawlinson & Kowadlo, 2017). Understanding the logic behind how things operate necessitates leveraging a wealth of contextual information, much like the human brain.

To augment the composite performance of machine learning across distinct scenarios and facilitate its real-world application in crucial decision-making, models specifically engineered to meet scenario-based demands have been developed in this chapter. Termed as scenario-specific or bespoke machine learning, this methodology entails a comprehensive examination of scenario peculiarities to furnish more targeted and customized solutions or services tailored to explicit requirements identified in practical contexts. The subsequent analysis in this chapter's summary will explore how these scenario-oriented machine learning models remediate the deficiencies found in conventional machine learning strategies.

### 5.1.2 Hypothesis

This chapter is founded on the hypothesis that: Guided by the dynamic information of the scenario, and with full consideration of the scenario's constraints and prioritized objectives, machine learning models customized for specific application scenarios can strike a balance between accuracy, efficiency, and adaptability, resulting in significant performance improvements. Unlike traditional general-purpose models, which prioritize generalization across a broad range of contexts, customized models address the nuanced requirements of individual cases and unique operational environments. This hypothesis builds on the premise that a deeper understanding of scenario-specific data, objectives, and constraints can lead to better model optimization and practical outcomes.

Through targeted customization, this chapter posits that machine learning models can:

Achieve superior predictive accuracy for both average cases and edge cases by tailoring algorithms and datasets to specific contexts. Balance resource consumption and

computational efficiency while maintaining high accuracy, even in resource-constrained environments such as large-scale medical screenings. Incorporate privacy, security, and interpretability into the design process to address user trust and ethical concerns.

### 5.1.3 Defining "Specific Requirements of The Application Scenario"

The "specific requirements of application scenarios" are defined as the specialized requirements that emerge within a particular operational environment or task context, focusing on the scenario's unique challenges, objectives, constraints, data characteristics, and user expectations (Giunchiglia, Imrie, van der Schaar, & Lukasiewicz; Kuwajima, Yasuoka, & Nakae; Mahmood, Huebner, & Reichenbach, 2023; Schuh, Scholz, Leich, & May; Vogelsang & Borg; X. Wang). These needs delineate detailed expectations for machine learning model metrics such as performance, efficiency, accuracy, interpretability, and security, as well as particular considerations regarding data type, volume, immediacy, and privacy safeguards.

**Environmental/Task Context.** This identifies the application domain or scenario from which these specific needs originate, such as healthcare, financial services, and intelligent manufacturing, among others. It incorporates the inherent patterns and knowledge of that scenario, forming its foundational logic (X. Chen, Singh, & Geyer; Dimitriadis & Goumopoulos; W. H, Hiromu, Foutse, Polytechnique, & Yann-Ga¨el; Nalchigar et al., 2019; Wörmann et al.). These may cover:

**Environmental Data.** Pertaining to environmental factors unique to the scenario, like geography, weather, and physical traits, these factors can have a significant impact on the decision-making process of the model (Aduri, Kuchipudi, & Prakash; Jubair & Domaratzki; Malakar; Varun; Zejnilovic et al.).

**Interaction Data.** Data derived from interactions between users and systems, including queries, responses, and feedback, are vital for enhancing user experience and model performance.

**Challenges and Objectives.** These detail the problems that need addressing within the scenario and the goals sought through machine learning technologies, which can vary

from improving predictive accuracy and reducing latency to elevating user satisfaction. The diversity in scenarios' challenges and objectives presents a significant challenge to traditional machine learning models' ability to comprehensively fulfill all requirements (Correia et al.; Gong, Zhong, & Hu; Horkoff).

**Constraints.** Addressing the restrictions that must be considered in the deployment of machine learning solutions, including computational resources, time, and legal compliance, underscores the necessity for multi-objective optimization strategies (Aickelin, Khorshidi, Qu, & Charkhgard; Akhter, Fährmann, Sonntag, & Peitz; Gardner et al.; Karl et al.; Preuveneers, Tsingenopoulos, & Joosen). This also implies requisite flexibility in the model concerning training resource management, duration, and sensitive data processing.

**Data Characteristics.** The importance of recognizing the distinctiveness of data within specific application scenarios—such as volume, variety (structured vs. unstructured), quality, and velocity—cannot be overstated (Gomes, Read, Bifet, Barddal, & Gama; L'Heureux, Grolinger, Elyamany, & Capretz; H. Liu, Gegov, & Cocea, 2017). Early consideration of these attributes in the modeling process enables bespoke adaptations to the data. A multifaceted approach to data includes: historical data, which encompasses past accumulations from analogous scenarios, essential for training models to discern patterns and trends (Din; X. L. Dong & Rekatsinas; H. Liu et al., 2017; Marlena; Rajaraman, Zamzmi, Yang, Xue, & Antani, 2023; Register; Sarah); real-time data, critical for models' timeliness and instant decision-making capabilities in numerous applications, requiring models to efficiently process current information (Nishihara et al.; Rajan et al.; Sasmal; D. K. Singh et al.; Singla et al.); and user behavior data, offering invaluable insights into user patterns, preferences, and feedback, thus facilitating model refinement to better meet user demands (Hal & Matija; Ojtáš & Peška; Sumaiya).

**User Expectations.** This concept pertains to end-users' anticipations regarding the machine learning model within the application scenario, which may cover aspects like ease of use, interpretability, and transparency. Such considerations afford a macroscopic evaluation of the model's overall efficacy, akin to the examination of "challenges" and "objectives," potentially serving to demystify the model's functionality for non-experts.

**Security and Privacy Protection.** There is a pronounced focus on safeguarding measures and privacy protections when processing sensitive information, especially pertinent in sectors such as healthcare and finance (Chandran, 2023; de Aguiar, Traina, & Traina; Javed, Muqeet, Javed, Rehman, & Sadiq; Runhua, N, & J; Shukla et al.; C. Zhang). In certain specialized industries, security or privacy benchmarks might be articulated through standardized, quantifiable formats. Moreover, ethical and legal constraints: adherence to prevailing legal statutes and ethical norms is imperative for any model customization, rendering these guidelines and stipulations essential inputs to guarantee compliance (Cannarsa, 2021; Drabiak, Kyzer, Nemov, & El Naqa; Paleyes, Urma, & Lawrence).

Conclusively, the specific needs of application scenarios elucidate the intricate and comprehensive criteria that a machine learning model must fulfill within a particular operational context, shaping the model's conception, development, and evaluative methods. Conducting research predicated on these scenario-specific requirements, coupled with tailoring models to the genuine conditions of these contexts, necessitates a broad engagement with relevant scenario data to ensure comprehensive learning and understanding of the scenario's intricacies. Through extensive incorporation of relevant data, models can more precisely grasp the scenario's unique aspects and demands, facilitating enhanced customization and optimization. This process boosts the model's generalizability and adaptability, enabling it to maintain efficacy and efficiency amidst evolving environments.

### 5.1.4 The Relationship Between Scenario Information and Individual Object Information

In the context of specific application scenarios, research unfolds under the demands of those scenarios, and model customization is conducted based on the objective conditions of the actual scenes. The scope of scene-related data that needs to be covered is extensive and depends on the application domain, task objectives, and specific business requirements

(Steven & T). These data are not isolated; scene data not only have internal complexities but also depend on and influence the information of individual objects (Herranz, Jiang, & Li; Khosla, Uhlenbrock, & Chen). Scene information provides the environmental background and conditions for individual objects, while the behaviors, states, and interactions of individual objects enrich and refine the content of the scene. This dynamic interaction is crucial for understanding the entirety of the scene and for effective model customization.

The relationship between scene information and individual object information can be generally categorized into three levels:

**Environmental Constraints and Individual Behavior.** Scene information provides environmental constraints for individual objects, such as geographic location, time, and environmental conditions. These constraints influence the behavior patterns and decision-making processes of individuals, affecting only a single individual (Cleveland, Robertson, & Volk; Cummiskey & Baer; F. D, J, & R; B. R. Newell, McDonald, Brewer, & Hayes; Vaeyens, Lenoir, Williams, Mazyn, & Philippaerts).

**Individual State and Scene Dynamics.** The state of individual objects (such as health status, mood, energy levels, etc.) influences their activities within the scene. In turn, these activities feedback into changes in the scene, affecting the states and behaviors of other individuals (Draschkow & Võ; Gagne & MacEvoy; Harari, Mars, Benoni, & Ullman; Kyriazis & Argyros). In other words, changes in an individual can propagate through the scene to other individuals.

**Interactions and Scene Evolution.** Interactions between individuals (such as communication, competition, cooperation, etc.) are key factors in the dynamic evolution of scenes (Congcong, Parikh, & Tsuhan; Harari et al.; Pirk et al.). These interactions not only shape the social structure of the scene but may also trigger scene-level events and changes, representing changes occurring at the scene level.

Considering the relationship between scenes and individual objects, analyzing scene

information can target enhancements in individual object performance. Analyzing the relationship between scene information and individual object information can serve the following purposes in model customization (Alamri & Pugeault; Bhat, Danelljan, Van Gool, & Timofte, 2020; K. Wu, Wu, & Kreiman; Yiyi, Kodagoda, Yue, Lei, & Yong):

**Enhance the model's contextual awareness.** By analyzing the relationship between scene information and individual objects, models can better understand and utilize context information for more accurate predictions and decisions. For instance, in recommendation systems, leveraging user environmental information and personal behavior data can provide more personalized recommendations (Ekstrand & Willemsen; Hashemi & Kamps; Jallouli, Lajmi, & Amous). When designing models, considerations for time series analysis and real-time learning algorithms are crucial to capture and utilize the temporal characteristics of data (Harika et al.; G. J; Misra & Siddharth; Q. Wen, Yang, Zhou, & Sun), enhancing the ability to parse diverse data types, including text, images, and sound. Utilizing multimodal learning approaches in model customization leverages the complementarity of different data types to improve the model's generalization capability and accuracy (Lu; W. Nan, Stanislaw, Kyunghyun, & Krzysztof; "R ECOGNIZING AND OVERCOMING THE GREEDY NA - TURE OF LEARNING IN MULTI - MODAL DEEP NEURAL NETWORKS," ; Huang Yu et al.).

**Improve model adaptability and flexibility.** Understanding the dynamic interplay between scenes and individuals helps design models that can adapt to environmental changes and changes in individual behaviors, thereby enhancing the robustness and flexibility of models in real-world applications. Employing dimensionality reduction techniques and deep learning models can effectively extract key features and reduce computational complexity (W. Jia, Sun, Lian, & Hou; Khalid, Khalil, & Nasreen; Velliangiri, Alagumuthukrishnan, & Thankumar joseph; Vij & Dalip), enabling models to handle high-dimensional data efficiently.

**Facilitate fine-grained model customization.** By deeply analyzing specific scene details and individual characteristics, models can be customized at a fine-grained level, designing more refined and personalized solutions for different user groups, environmental

conditions, or task requirements. In certain application scenarios, where the distribution of positive and negative samples is extremely imbalanced, addressing the minority class group with oversampling, undersampling techniques, or designing specific loss functions to handle sample imbalance issues is essential (Goswami & Roy, 2020; Jairo & P; Mahmoud, El-Kilany, Ali, & Mazen; Pattanayak & Rout, 2017; Rozianiwati, K, A, N, & N; Watthaisong, Sunat, & Muangkote).

**Strengthen model interpretability, transparency, and robustness.** Clarifying the mechanisms of interaction between scene information and individual behavior enhances model interpretability, making the decision-making process and prediction results more transparent and trustworthy for end-users. Applying data cleaning and anomaly detection techniques to improve data quality and designing robust models to reduce the impact of noise are crucial steps to mitigate the influence of real-world data noise (Chiara, Federica, & Laura; Chong & R; Farzaneh, Zhewen, & Vitor; Ki, Yuji, Young, Hyunsub, & Steven; García S, Julián, & Francisco; Zilong et al.).

In summary, analyzing and understanding the relationship between scene information and specific objects within a scene is highly beneficial for model customization. This not only enhances model performance and efficiency in specific scenarios but also ensures that model designs are closer to real-world application needs, meeting the specific expectations of users.

### 5.1.5 Leveraging Specific Scenario Requirements for Model Customization

Customizing models for specific application scenarios necessitates the comprehensive utilization of scenario-related data to enhance model performance. The following structured methodology is designed to optimize model design and performance through a deep understanding and integrated use of scenario data:

**Understanding and Defining Scenario Requirements**

Identifying Scenario Objectives and Constraints. Initially, it is crucial to have a clear

understanding and definition of the specific requirements of the application scenario. This includes the problems to be solved, the objectives of the scenario, and any existing constraints (such as time, cost, resources, etc.). Recognizing Key Data Elements. Based on the scenario's requirements, it is important to identify which data elements are critical. These may include environmental data, individual behavior data, interaction data, and more.

**Collecting and Analyzing Scenario-related Data**

Data Collection. In alignment with the defined data elements, collect as comprehensive a dataset as possible related to the scenario. This may involve field measurements, online tracking, database queries, and other methods. Data Preprocessing and Analysis. Preprocess the collected data, which includes cleaning, normalizing, feature extraction, etc., and then conduct preliminary data analysis to understand the basic characteristics and patterns of the data.

**Model Design and Customization**

Selecting or Designing Model Architecture. Choose or design an appropriate machine learning model architecture based on the specific requirements of the scenario and the characteristics of the data. This may involve traditional machine learning algorithms, deep learning models, or other advanced models. Utilizing Data Characteristics. In designing the model, make full use of the characteristics of the data. For example, employ time-series analysis techniques for data with strong temporal properties, adopt multimodal learning approaches to integrate different types of data, or use specific algorithms to handle high-dimensional data and address sample imbalance issues.

**Model Training and Optimization**

Model Training. Utilize the collected data to train the model. During this phase, multiple iterations may be necessary to adjust model parameters and training strategies to achieve optimal learning outcomes. Model Optimization. Based on preliminary training results, further optimize the model. This may involve tuning hyperparameters, improving feature engineering, and adjusting the model structure.

**Validation and Deployment**

Model Validation. Validate the model using an independent test set to ensure its performance on unseen data is satisfactory. Given the complexity of real-world application scenarios, field testing or A/B testing (A/B testing, also known as split testing, is a method used in experimental research and decision-making to compare two variants (A and B) to determine which performs better.) may also be necessary. Model Deployment and Monitoring. After achieving satisfactory validation results, deploy the model in the actual application scenario. Post-deployment, continuously monitor the model's performance and make necessary adjustments and optimizations based on feedback.

Through this series of structured steps, it is ensured that machine learning models can not only fully leverage scenario-related data to enhance performance but also closely align with the needs of real-world application scenarios to achieve optimal results in practical applications. Customizing models under specific scenario requirements necessitates a deep understanding of the characteristics of scenario-related data. This requires not only a thorough understanding of the data itself but also a comprehensive grasp of the application scenario, business logic, and end-user needs. Throughout the process, the key to success lies in valuing the quality and characteristics of data, the interpretability and adaptability of the model, and its close integration with the actual application scenario.

## 5.2 The Case for Research

### 5.2.1 A Brief Description of The Application Scenario

At the 77th session of the United Nations General Assembly, the World Health Organization (WHO) emphasized non-communicable diseases (NCDs) as the most pressing health and development challenges of the 21st century. Concurrently, they released a report titled "Invisible Numbers. The True Extent of Non-Communicable Diseases and What to Do About Them (Organization, 2022)". The report offers stark data on NCDs, encompassing conditions such as heart disease, cancer, and diabetes, among others. Annually, these diseases account for 41 million deaths, with cardiovascular ailments

being the leading cause.

Cardiovascular diseases (CVDs) stand as the foremost cause of global mortality, surpassing all other diseases. CVDs account for approximately one-third of all deaths worldwide, with 17.9 million fatalities annually (World Health Organization, 2020). Encouragingly, with effective prevention and treatment, a significant proportion of CVD deaths can be either prevented or delayed. Some reports suggest that up to 86% of these fatalities could be averted (Murray et al., 2020; Roth, 2018). The authors contend that bolstering investments in non-communicable disease (NCD) prevention and treatment, especially in low-and-middle-income countries (LMICs), could yield a significant positive impact by 2030. The authors posit that an annual investment of USD 18 billion in LMICs could manifest a net economic benefit of USD 2.7 trillion within the ensuing seven years (Countdown, 2022). Such a commitment should be viewed more as an investment than a cost, given that the derived benefits would transcend just health outcomes. To harness these advantages, the World Health Organization advocates for stronger healthcare delivery systems. This ensures effective NCD prevention, detection, and treatment and provides targeted support to vulnerable populations most susceptible to NCDs.

Owing to prevalent psychological tendencies, most individuals are more attentive to and take explicit health risks more seriously. Therefore, to mitigate heart-related disease risks, it is imperative to inform patients about their diagnosis, the disease's progression, and the associated risks. While early diagnosis might not guarantee a complete cure for heart disease, adopting healthy lifestyle habits and receiving appropriate treatment can significantly diminish mortality risks and enhance the quality of life (Ornish et al., 1990).

This context necessitates governmental efforts for large-scale screenings among high-risk groups, ensuring patients are informed early about potential risks. A notable distinction between large-scale screenings and conventional hospital-based testing is the associated labor and time costs. Indeed, physician resources might be inadequate to manage detailed diagnoses for expansive populations (Wilson, Jungner, & Organization, 1968). Concurrently, the lengthy and cumbersome process can deter the general populace from participating, posing a challenge to successful large-scale screenings (Holland & Stewart,

2018; Rembold, 1998). For effective large-scale heart disease screenings, the testing process must be non-invasive, straightforward, and swift. It should leverage instruments that can be readily scaled up, while a critical aspect remains minimizing human intervention.

Based on the practical requirements discussed earlier, analyzing data from large-scale screenings necessitates the use of an appropriate and potent tool. Consequently, numerous researchers have investigated self-assessment using digital tools, like machine learning, enabling individuals to analyze their own data on personal devices (Frost, Doryab, & Bardram; R. Kumar, Singh, Sahoo, Das, & Jha, 2023; R. Sharma & Rani; Z. Yin, Sulieman, & Malin). Contemporary mainstream general-purpose machine learning models predominantly require vast datasets for training. They improve their generalization capabilities through techniques like data augmentation. Nevertheless, recent advancements in machine learning primarily focus on exploring unstructured data in intricate scenarios. These advanced deep learning techniques often fall short when handling structured data (Borisov et al., 2022; Shwartz-Ziv & Armon, 2022). Given that large-scale screenings predominantly yield structured data, deep learning does not emerge as an optimal choice for this purpose.

Moreover, current machine learning models present evident ethical challenges when applied to medical problems (Guraya, London, & Guraya, 2014). Traditional machine learning often employs averaging to gauge model performance, potentially masking disparities in individual outcomes (Chouldechova A & M; G. B, Charles, Mélanie, & S; Pfohl, Foryciarz, & Shah). While a model might excel on average with a validation set, and subsequently show strong generalization on untrained test sets, this does not guarantee uniform excellence. Disturbingly, once a general-purpose model is trained, its determinations about patient outcomes are essentially fixed (Beaulieu-Jones et al.; Bilwaj, Kirstin, Luke, Eb, & Ai; D'Hondt, Ashby, Chakroun, Koninckx, & Wuyts; Sutter, Roth, Chin-Cheong, Hug, & Vogt; Vaid et al.). Regardless of whether it evaluates ten or a hundred thousand individuals, the model's parameters remain static, because by the end of the training phase, the model has reached its limit in terms of average performance. This rigidity means that certain patients will invariably be misdiagnosed. Who would willingly

be that “unfortunate patient” misdiagnosed by the model? It is distressing for any patient to contemplate that they might have been inadvertently overlooked during the model’s inception. Each data sample processed by the model directly corresponds to a patient. In fact, a disease diagnosis is not merely a classification task on data; it has profound implications for real, living individuals (Siegler, Pellegrino, & Singer, 1990; Veatch, 1997). Given these ethical concerns, the primary goal in tailoring diagnostic models for individuals should be achieving the utmost accuracy. The pursuit of optimal model accuracy entails not only a focus on the model’s average performance, but also a commitment to ensuring acceptable performance in the most challenging cases. Through the foregoing analysis, it is deduced that to harness the optimal utility of machine learning in large-scale disease screening, customize models based on each patient’s specific circumstances represent a potentially viable approach. This one-person-one-model approach has already been shown to be excellent in the previous chapter. The situation at this point is different from the previous chapter's scenario. Hepatitis C’s detection in hospitals can be considered only to pursue the highest accuracy. However, if we want to apply customised machine learning to large-scale screening for heart disease, prediction accuracy is not the only goal to be pursued; resource consumption and efficiency are also factors that must be considered (Alan, A, James, Johanna, & V; Connor, S, & H; "Machine Learning under Resource Constraints - Volume 3: Applications," ; Pengtao; Raghavendra,

Julian, & Erik; Renyu, Ouyang, Yaofeng, P, & Jie; Zhenge et al.).

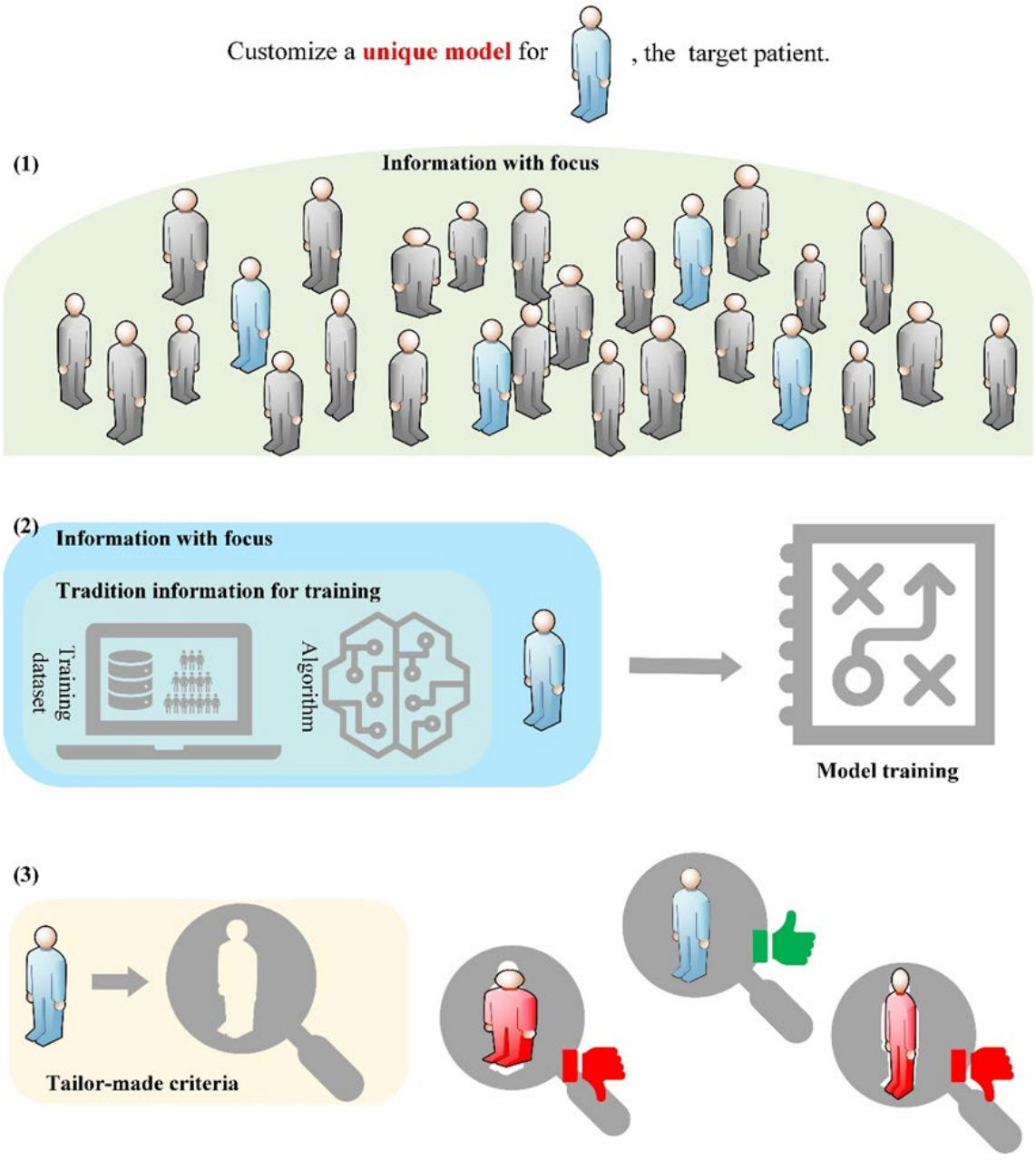



*Figure 22. Conceptualization schematic.*

Note: (1) Data processing level: Select the information worthy of attention from a large amount of information to focus on; (2) the neural network design level: Introduce attention mechanism in the model training process; and (3) the model evaluation level: Customized evaluation criteria for each patient

This study aims to fill this research gap by investigating the feasibility of custom

solutions. This chapter hypothesizes that diagnostic models, when customized according to individual information, may enhance diagnostic accuracy. And with full consideration of the realities of the application scenario, a customised solution can strike a balance between multiple criteria. This chapter anticipates that by judiciously crafting models, customized to specific patients, more accurate detection results can be achieved without a significant alteration in the number of model parameters. In the exploration to realize model customization, this chapter attempts to incorporate individual information at various stages of model development, aspiring to achieve tailored machine learning models. And in each process, according to the requirements of the scenario, privacy protection considerations and the full and timely use of new data are carried out (Q. A, Junaid, M, & Ala; Aasheesh et al.; Aycan, Tizian, Maike, S, & L; Guerra-Manzanares, Lopez, Maniatakos, & Shamout, 2023; Mohandas, Veena, Kirubasri, Mary, & Udayakumar; Shakira et al.; Wonsuk & Junhee; Xin, Fariza, Zongwen, & S). Several customized operations and functional iterations are proposed at the data processing level, the neural network design level, and the model evaluation level, as shown in Figure 22.

### 5.2.2 Dataset and Preprocessing

For effective large-scale disease screening, it is essential that dataset features are collected efficiently, cost-effectively, and with minimal time consumption. In this chapter, the Cleveland heart disease dataset (Detrano, 1988), the most frequently selected dataset in heart disease research, and a combined dataset of five heart disease datasets from the UCI machine learning repository dataset (Andras Janosi, 1988) (including the Cleveland dataset) are selected to validate the applicability of the custom machine learning algorithm for large-scale detection.

**Cleveland Heart Disease Dataset**

The Cleveland Heart Disease Dataset comprises 303 instances, each representing an individual patient. It includes 13 unique attributes that serve as informative factors in determining the presence of heart disease. These attributes primarily encompass results from non-invasive diagnostic examinations, along with other relevant patient-specific details. The target variable of interest pertains to the outcomes derived from invasive coronary angiography, which serves as a reliable indicator for identifying the presence or

absence of heart disease. The target variable assumes binary values, with the value '0' denoting an absence of heart disease, while the value '1' indicates the presence of heart disease. See Table 10 for a description of the dataset.

**UCI Machine Learning Repository Dataset**

The dataset is created by combining five separate heart disease datasets. The combined dataset initially had 1190 observations from five sources: Cleveland (303), Hungarian (294), Switzerland (123), Long Beach VA (200), and Stalog (Heart) (270). After removing 272 duplicated instances, the final dataset contained 918 observations. The dataset comprises 11 common features, with the exception of the Cleveland dataset, which contains additional Ca and Thal features, rendering it the largest dataset of its kind available for research purposes.

Ethical considerations were taken into account during the collection and use of data. All the data used in this research were acquired from publicly accessible sources and appropriately cited following the data publishers' requirements (Andras Janosi, 1988; Detrano, 1988). Additionally, to safeguard patient privacy, any identifying patient information was either anonymized or removed by the data publisher.

This chapter conducted exploratory data analysis to verify the dataset's quality and reliability. The pandas (McKinney, 2011) and NumPy (Oliphant, 2006b) functions were used to carry out initial data assessment and to identify any missing or abnormal values. The meaning behind each feature was meticulously scrutinized to detect any values that fell outside the expected range or that conveyed meaningless information. The publicly available dataset used here was reviewed by researchers with a background related to medical knowledge and had no obvious outliers. Since the processing of missing data values will introduce new errors, this chapter opted to remove instances containing missing values. After removing entries with missing values, the Cleveland dataset sample had 297 observations, of which 137 were confirmed patients. Similarly, the UCI combined dataset sample had 746 observations, with 356 confirmed patients. To mirror large-scale detection scenarios, this chapter preserved the datasets in their rawest form, avoiding feature engineering, outlier removal, or data augmentation for specifically labeled samples. Tables 11 and 12 provide further information and analysis of the data.

Table 10. Description of the dataset.

| no. | Data type | Attributes | Description |
|---|---|---|---|
| 1 | Numeric | Age | It is described in years |
| 2 | Binary | Sex | Gender where 1 represents male while 0 represents female |
| 3 | Categorical | Chest pain (CP) | It is type of chest pain having four classes with varying degree |
| 4 | Numeric | Resting blood pressure(restbps) | Measure of blood pressure in mmHg |
| 5 | Numeric | Cholestoral (chol) | Measure of serum cholestoral in blood |
| 6 | Binary | Fasting blood sugar (fbs) | Measure of sugar in blood with fasting |
| 7 | Categorical | Resting ECG (restecg) | Measure of ECG in resting phase having three classes: normal, ST defected, and ventricular hypertrophy |
| 8 | Numeric | Thalach | Maximum heart rate in beats per minute |
| 9 | Binary | Exang | Exercise-induced angina |
| 10 | Decimal | Old peak | ST depression induced by exercise |
| 11 | Ordinal | Ca | Number of major vessels colored |
| 12 | Categorical | Thal | Represents thallium stress test results (0 = NA, 1 = fixed defect, 2 = normal, 3 = reversible defect) |
| 13 | Categorical | Slope | The slop of ST segment having three classes, upward, flat, and downward slopes with values of 0, 1, and 2 |
| 14 | Binary | Target | Target attributes having two classes where 1 indicates presence of heart disease, 0 indicates absence of heart disease |

Table 11. Basic information and analysis of the Cleveland dataset

| Attributes | Average | Median | STE | STD | Range |
|---|---|---|---|---|---|
| Age | 54.54 | 56 | 0.53 | 9.05 | [29,77] |
| Sex | 0.68 | 1 | 0.03 | 0.47 | [0,1] |
| CP | 3.16 | 3 | 0.06 | 0.96 | [1,4] |
| RestBPS | 131.69 | 130 | 1.03 | 17.76 | [94,200] |
| Chol | 247.35 | 243 | 3.02 | 52.00 | [126,564] |
| FBS | 0.14 | 0 | 0.02 | 0.35 | [0,1] |
| RestECG | 1.00 | 1 | 0.06 | 0.99 | [0,2] |

| Attributes | Average | Median | STE | STD | Range |
|---|---|---|---|---|---|
| Thalach | 149.60 | 153 | 1.33 | 22.94 | [71,202] |
| ExAng | 0.33 | 0 | 0.03 | 0.47 | [0,1] |
| Oldpeak | 1.06 | 0.8 | 0.07 | 1.17 | [0,6.2] |
| Ca | 1.60 | 2 | 0.04 | 0.62 | [13] |
| Thai | 0.68 | 0 | 0.05 | 0.94 | [0,3] |
| Slope | 4.73 | 3 | 0.11 | 1.94 | [3,7] |
| Target | 0.46 | 0 | 0.03 | 0.50 | [0,1] |

Table 12. Basic information and analysis of the UCI combined dataset

| Attributes | Average | Median | STE | STD | Range |
|---|---|---|---|---|---|
| Age | 52.88 | 54 | 0.35 | 9.51 | [28,77] |
| Sex | 0.76 | 1 | 0.02 | 0.43 | [0,1] |
| CP | 0.84 | 1 | 0.03 | 0.96 | [0,3] |
| RestBPS | 133.02 | 130 | 0.63 | 17.28 | [92,200] |
| Chol | 244.64 | 237 | 2.17 | 59.15 | [85,603] |
| FBS | 0.17 | 0 | 0.01 | 0.37 | [0,1] |
| RestECG | 0.64 | 0 | 0.03 | 0.84 | [0,2] |
| Thalach | 140.23 | 140 | 0.90 | 24.52 | [69,202] |
| ExAng | 0.38 | 0 | 0.02 | 0.49 | [0,1] |
| Oldpeak | 0.90 | 0.5 | 0.04 | 1.07 | [-0.1,6.2] |
| Slope | 0.99 | 1 | 0.04 | 0.97 | [0,2] |
| Target | 0.48 | 0 | 0.02 | 0.50 | [0,1] |

### 5.2.3 Related Work

This section provides an overview of machine learning classification methods related to structured data from heart disease in recent years, and conducts a comprehensive analysis and comparison at the data level and algorithm level, respectively. It focuses on the analysis of the different results presented for the same dataset (Ahsan & Siddique, 2022).

**Data Level**

The main forms of improving classification accuracy at the data level are imbalanced data processing and feature engineering. Jesmin Nahar et al. (Nahar, Imam, Tickle, & Chen, 2013) developed a medical knowledge-driven feature selection process (MFS) and investigated MFS combined with the computerized feature selection process (CFS). Wiharto et al. (Wiharto, Kusnanto, & Herianto, 2016) used resampled non-stratified random sampling, the synthetic minority over-sampling technique (SMOTE) for unbalanced datasets to effectively mitigate the accuracy impact of unbalanced data. The Similarity-based attribute weighting methods via clustering algorithms proposed by Kemal Polat (Polat, 2018) obtain better classification performance in the handling of classifying the imbalanced medical datasets than the random subsampling method. Gan et al. (Gan, Shen, An, Xu, & Liu, 2020) proposed an integrated TANBN with a cost-sensitive classification algorithm (AdaC-TANBN), which employs variable misclassification cost determined by samples distribution probability to train a classifier, and not like in past work searching for an excellent classifier to maximize classification accuracy with the fixed misclassification cost. Finally, it achieved 80.27% accuracy rate and 88.87% area under the curve (AUC). In terms of data processing, the degree of innovation in recent years is not high and homogenization is more serious. It is basically limited to improving the accuracy of the model through data augmentation or feature-level processing.

**Algorithm Levels**

Devansh Shah et al. (D. Shah, Patel, & Bharti, 2020), and K. Deepika et al. (Deepika & Seema, 2016) compared the performance of multiple traditional classification algorithms on the Cleveland heart disease dataset. CBC Latha et al. (Latha & Jeeva, 2019) used ensemble learning to combine the results of multiple algorithms and eventually achieved 85.48% accuracy; similarly, Amin et al. (Amin, Chiam, & Varathan, 2019) achieved 87.41% accuracy using multi-model voting.

A. K. Paul et al. (Paul, Shill, Rabin, & Akhand, 2016; Paul, Shill, Rabin, & Murase, 2018) proposed a genetic algorithm-based fuzzy decision support system for predicting the risk level of heart disease, which is an attempt at a Neural network with fuzzy logic. The Recurrent Neural Network (RNN)+ Long Short Term Memory (LSTM) developed by Surenthiran Krishnan et al. (Krishnan, Magalingam, & Ibrahim, 2021) is a refreshing form

of structured datasets, but there is less subsequent related research in this direction.

Progress in the field of algorithms also lacks new directions and is still mainly limited to the traditional means of structured data processing, squeezing the performance limits of traditional classifiers by means of parameter optimization or multi-model fusion. Perhaps customized processing will be a brand-new path in this field.

## 5.3 The Specific Requirement of Large-Scale Disease Screening

The deployment of large-scale disease screening models necessitates a nuanced understanding of the specific requirements inherent to this application scenario. These requirements encompass several critical dimensions, as outlined below:

Efficiency and Scalability: Screening models must demonstrate high efficiency and scalability to process vast datasets derived from the target population. This entails the ability to handle structured data from large-scale screenings, including patient demographics, clinical parameters, and diagnostic test results, with minimal time consumption and computational resource requirements.

Accuracy and Sensitivity. Given the high stakes involved in disease detection and diagnosis, screening models must exhibit exceptional accuracy and sensitivity. This is crucial for ensuring that high-risk individuals are accurately identified for further investigation or intervention, thereby minimizing the risk of false negatives that could lead to delayed treatment.

Adaptability and Customization. The dynamic nature of disease epidemiology and patient populations necessitates that screening models are adaptable and customizable. Models must be capable of incorporating new data and evolving based on emerging disease patterns, patient demographics, and environmental factors influencing disease prevalence and manifestation.

Ethical Considerations and Data Privacy. Large-scale screening initiatives involve the processing of sensitive personal and health information. Therefore, screening models must adhere to stringent ethical guidelines and data privacy regulations, ensuring the protection of individual patient data and confidentiality throughout the screening process.

Interdisciplinary Integration. Effective disease screening models require the integration of interdisciplinary knowledge, combining insights from medical science, data science, epidemiology, and public health. This interdisciplinary approach is essential for developing models that are not only technically robust but also grounded in clinical relevance and public health priorities.

## 5.4 Specific Solutions

This section delves into the process by which custom machine learning algorithms enable models to be tailored to individual patients, considering specific problems. The customized operation is mainly performed in three stages: data processing, neural network structure design, and model evaluation. Beyond analyzing and justifying the proposed methodologies from a data science viewpoint, this chapter seeks to explore their validity through a more intuitive discussion.

### 5.4.1 Data Augmentation with Focus

For data engineers, a rich, comprehensive, and sufficient amount of data is an indispensable prerequisite for training a well-performing machine learning model (Flach, 2012). However, the criteria defining an effective model shift with varying application scenarios. Thus, broad criteria may not apply directly to a particular problem. Traditional general-purpose machine learning models, aimed at replacing humans in large-scale repetitive decision-making, prioritize better generalization and higher overall accuracy (Bousquet & Elisseeff, 2002). However, this goal is cruel in the eyes of those individuals being decided, because no one cares about those few individuals whose information is not considered by the model. To ensure each individual's diagnosis is favored, custom machine learning algorithms should have evaluation criteria aligned with the individual's specific scenario. When the model's evaluation criteria overlook aspects like overfitting and generalization (Bousquet & Elisseeff, 2002), the rationale behind the composition of the training set also shifts.

Another issue to consider is that the medical problems dataset is particularly specific because of the presence of difficult miscellaneous diseases (Van Der Bom et al., 2011). Patients with such conditions pose inevitable challenges throughout a physician's career,

presenting distinct data within the broader dataset. In the training process of traditional machine learning models, such unique samples, which are distinct from other samples and small in number, cannot have a significant impact on the overall training direction of the model. This underrepresentation of specific patient profiles means general-purpose machine learning models frequently struggle to analyze those with difficult miscellaneous diseases accurately. If algorithms like SMOTE (Synthetic Minority Over-sampling Technique) (Chawla et al., 2002; Deepika & Seema, 2016; Pradipta, Wardoyo, Musdholifah, Sanjaya, & Ismail, 2021) augment this sparse unique data, it will greatly reduce the accuracy of the model for ordinary patients with limited improvement in the accuracy of the judgment of patients with difficult and complicated diseases, which is not worth the loss (Naseriparsa, Al-Shammari, Sheng, Zhang, & Zhou, 2020).

At this point, the complexity of the particular needs of the scenario comes into play. With a large sample of data, we need to get a high accuracy rate for the vast majority of people, but also allow a few difficult patients to be treated with some focus. At this point, how to design the training set becomes an adjustment. The training set needs to be flexible according to the distribution of the data of the people to be detected in the sample space.

To address this challenge, this chapter proposes a custom machine learning algorithm in this study that crafts a distinct training set for each patient during the data processing phase. This specialized training set is exclusively employed for the designated target patient, ensuring no influence on other patient models. To ensure comprehensive learning of the target patient's features, this study also accounts for patient similarities and the relative standing of a target patient's test outcomes within the range of variation. Similar patients have similar test results, and data augmentation for similar patients helps the model to be more sensitive to data within the interval of the target patient's test results. The proposed "data augmentation with focus" employs the SMOTE algorithm, generating samples closely resembling the target patient. The SMOTE algorithm, an interpolation-based method, crafts new samples for underrepresented classes, thereby enriching the dataset's representativeness. The graph of data augmentation with focus versus traditional data augmentation is shown in Figure 23.

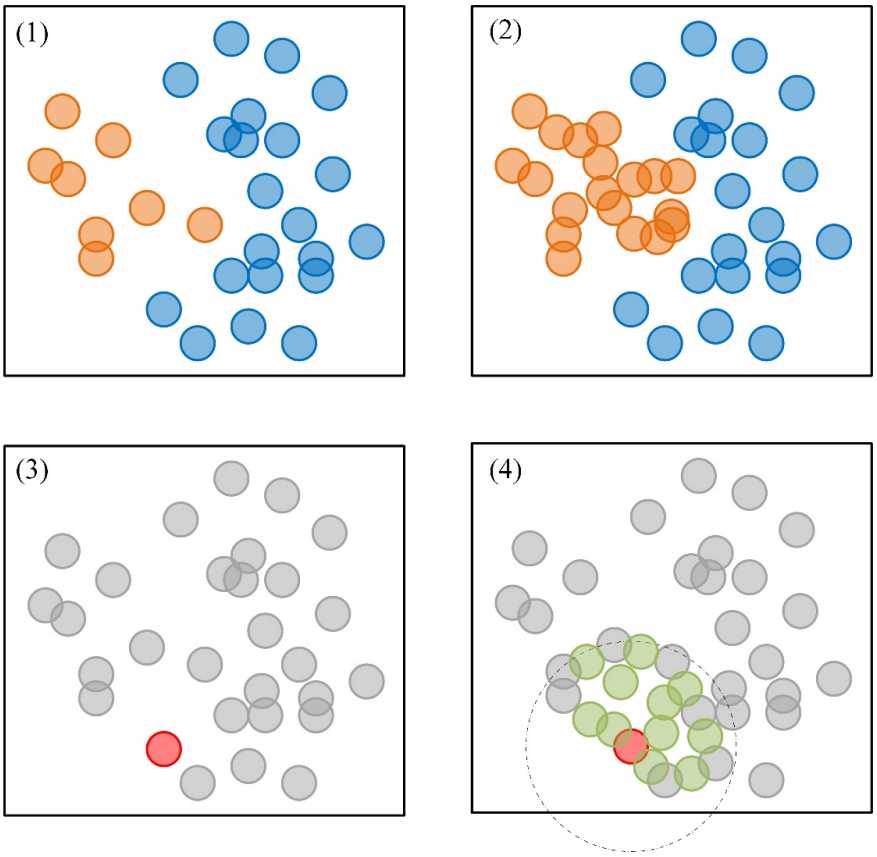



*Figure 23. Comparative Analysis of Data Augmentation Effects.*

Note: (1) & (2): Traditional data augmentation process. The (1) illustrates imbalanced data without the SMOTE algorithm's augmentation. The (2) displays results post data processing. (3) & (4): Data augmentation with focus. Unlike traditional methods, the process does not rely on the class of the sample. Here, only the red target sample is of concern. The (3) highlights the target before augmentation, while the (4) demonstrates augmentation exclusively around the target. The dashed line indicates the similarity threshold.

For the selection of the scale criteria for measuring patient similarity, several measures commonly used in the field of data science were compared and experimented with the following results, as shown in Figure 24.

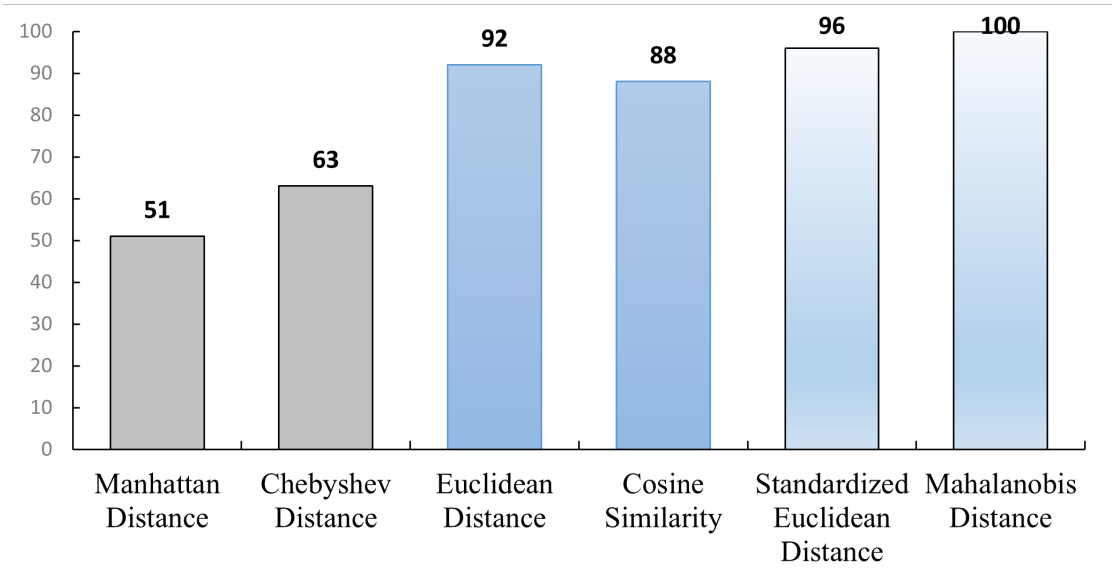



*Figure 24. Comparison chart of the accuracy brought by different distance calculation methods.*

Note: The effectiveness of the various distance calculation methods is scored based on the combined performance of the Mahalanobis distance in the custom model.

Finally, the best-performing Mahalanobis distance (De Maesschalck et al., 2000) was selected as the metric to measure the similarity between different patients. The equations for calculating the Mahalanobis distance are as follows:

$$\bar{x} = \frac{1}{M}\sum_{i=1}^{M} x_i \tag{40}$$

$$S = \frac{1}{M-1}\sum_{i=1}^{M}(x_i - \bar{x})(x_i - \bar{x})^T \tag{41}$$

$$D(x_i, x_j) = \sqrt{(x_i - x_j)^T S^{-1}(x_i - x_j)} \tag{42}$$

In equation (40), M is the number of samples in the dataset, $\bar{x}$ is the mean of the samples, which is a column vector, and $x_i$ is the i-th sample, which is also a column vector. $D(x_i, x_j)$ in equation (42) is the Mahalanobis distance between $x_i$ and $x_j$.

After determining how to measure the degree of similarity, the next step is to augment the data with an appropriate number of similar samples. This requires setting a threshold to oversample the very similar samples with similarity above the threshold by the SMOTE algorithm: **similarity threshold**. After preliminary experiments with different thresholds,

the best results are obtained when the **similarity threshold** is set to about one-third of the number of sample features (sample space dimension). The dataset continues to expand with the gradual implementation of large-scale screening. The sample density of the sample space also increases slowly. When the number of samples satisfying the augmentation threshold is always too many without augmentation, the similarity threshold can be appropriately lowered before augmentation.

In addition to being related to the sample dimensions, the setting of the similarity threshold is also related to the amount of training set data used. Each of these hyperparameters needs to be adjusted based on information other than the samples in the field. This also reflects the importance of fully understanding the particular needs of the scenario. Since the SMOTE algorithm requires at least six samples as the basis for oversampling, sometimes some special target patients cannot find six samples in the test set with the Mahalanobis distance below the similarity threshold. The strategy adopted in this case is to not perform sample augmentation and to label these patients lacking similar samples. This marking is a reflection of the seriousness with which each patient is treated. Once a person to be tested is found to have data so rare that fewer than six people resemble him or her. Such a person should receive a more detailed medical examination.

Another critical parameter in the SMOTE algorithm is the "**augmentation threshold**", representing the proportion of minority class samples after oversampling. At this stage, the oversampled minority class samples are those closely resembling the chosen target patients. The SMOTE algorithm augments the number of samples in the minority class until the ratio of the number of samples in the minority class to the number of samples in the majority class (those considered less similar) reaches the augmentation threshold. The range of the augmentation threshold can be set between 0.3 and 0.8, and the different settings help the model to use different parameters depending on the distribution of samples in the data set. If the sample proportion slated for augmentation surpasses the augmentation threshold even before the process begins, no further augmentation is necessary. Depending on the needs of large-scale disease screening, this threshold cannot be static. This threshold should be set in such a way that it decreases gradually as the samples in the training set increase.

In order for the custom model to be more focused on patient analysis, it can actually

also perform feature engineering on a certain number of test results data with distinct characteristics of the target patient. This helps the model select effective, appropriately sized features, which in turn allows the model to perform its task effectively and efficiently. Good feature engineering relies on the data engineer's deep understanding of the operational content. Nevertheless, as this study seeks to present a standard model with minimal human intervention, we've opted not to delve into advanced feature engineering that necessitates a specialized knowledge base.

### 5.4.2 Neural Networks with Attention

Since the content of this section is basically the same as the functional feature design in the previous chapter, this section in this chapter mainly clarifies why such a design is necessary through logical analyzes.

How to express the goal of customization in the design of neural network structure is a rather abstract problem, so let's think about this problem in another way. At its core, training a machine learning model involves iterative calculations over myriad samples. By adjusting data flow and meticulously crafting computation rules, this chapter translates these abstract concepts into tangible solutions. In order to make the trained custom model more sensitive to specific patients, it is necessary to let the model know which patients are to be given special attention, i.e., to receive data from the target patients during the training process. It is important to note that the target patient data contains only laboratory results but not diagnostic results, so this data is different from the historical data in the training set that has both laboratory and diagnostic results.

Bearing this unique data input requisite in mind, this chapter reexamines the model's training process. During the model's training phase, it ingests batches of sample data, processing them in parallel within the neural network, leading to expected outcomes via computations across each node and layer (Da Silva et al., 2017). The results of the loss function are calculated and used to guide the updating of the weight parameters in the neural network. In this process, the samples in each batch are passed into the model sequentially according to the random positions in the training set, so this process cannot produce specificity to particular data. In the subsequent flow of data between different layers of the neural network, it is a tricky problem to adapt the dimensionality of patient

test results data to the dimensionality of each layer in the neural network if the data of a particular patient is incorporated as special additional information in any layer. At the same time, the repeated use of such fixed noise-like data across multiple layers will cause gradient explosion or disappearance under the influence of the chain rule, making the model training process unsustainable.

With the constraints of the above analysis, integrating target patient information into the model necessitates the addition of a distinct neural network layer immediately following the input layer. This approach ensures consistent dimensionality and enables one-to-one correspondence processing for data of the same dimension. Additionally, it allows for the seamless integration of extra information in a single pass, without disruption to subsequent modules of the standard neural network.

After determining the location of the new functional module of the model, the next step is to design the specific functions of this particular neural network layer. The attention mechanism is one that allows the model to give higher attention to key information at certain moments, while reducing the impact on other information (Vaswani et al., 2017a). While attention mechanisms are typically employed to emphasize specific features or localized sample information, they are seldom used to highlight disparities between samples. In this study, this chapter designed a focused attention mechanism within the neural network, drawing inspiration from existing attention methodologies and leveraging the target patient's data as pivotal information (refer to Figure 25). This is top-down attention that has a predetermined purpose, is task-dependent, and actively and consciously focuses on an object. The concrete measure is to add a special attention layer after the input layer to superimpose the target patient's lab data with the data from each incoming training set. That is, an $x_t \cdot (e - e')$ is added to each individual data $x_i$ in the data batch transferred from the input layer to the attention layer.

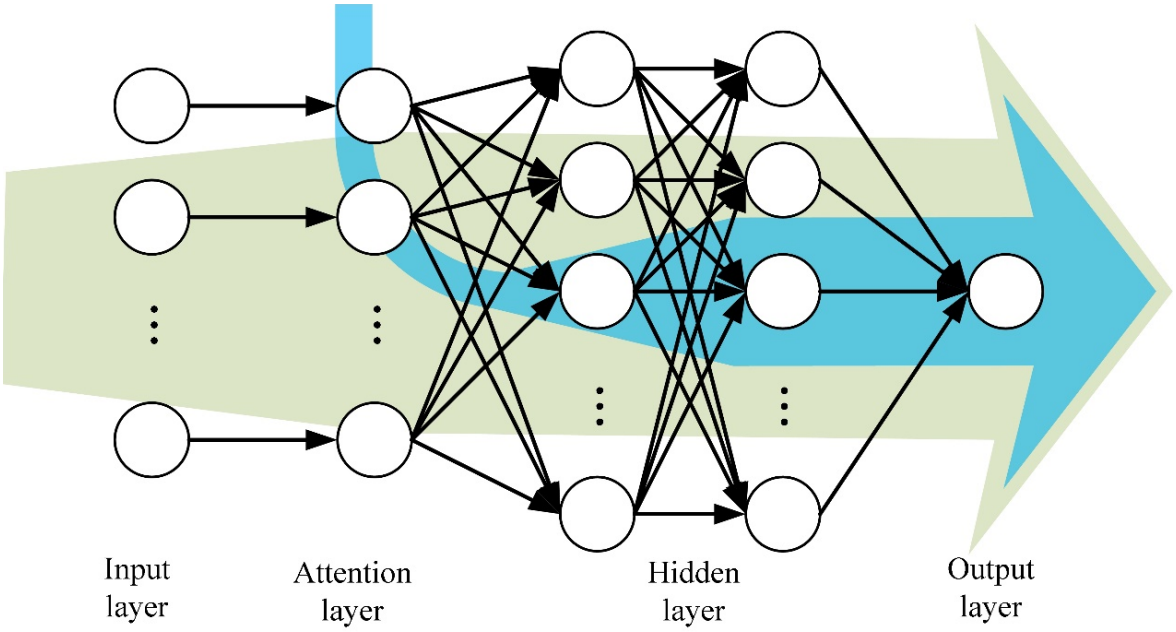



*Figure 25. Schematic diagram of the model structure.*

Note: The green arrow represents a large amount of training set data that is sequentially passed into the model during training, and the blue arrow represents the target patient data that is passed into the model, which is only a small amount of data but still plays a significant role in the model computation.

Setting the scaling factor of $x_t$ to the two-parameter form of $(e - e')$ is carefully designed. These two coefficients are **bias coefficient** $e$ and **restore coefficient** $e'$ respectively. **Bias coefficient** $e$ is a pre-determined artificial fixed offset coefficient that expresses the magnitude of the initial attentional influence. **Restore coefficient** $e'$ is a parameter that can be continuously trained by the bp algorithm and will be continuously adjusted during the training of the model, which expresses that the model continuously corrects the attentional influence by the change of the loss function during the training process. After such a calculation, the data passed into the subsequent hidden layer becomes $x_i + x_t \cdot (e - e')$.

The modified data input to the subsequent neural network can be described in two ways, namely:

1) The training data passed to the subsequent network, which is considered by the model as a golden rule for self-tuning, is the laboratory results of one historical patient

superimposed on the laboratory data of a target patient scaled by a coefficient of $(e - e')$. In other words, each historical patient's data learned by this model contains a weak noise that is closely related to the target patient (Atla et al., 2011), with a noise size of $x_t \cdot (e - e')$, as equation (43). This noise is sometimes large and sometimes small throughout the training process ($e'$ is constantly changing). At this point, the goal of machine learning model training is to find a stable mapping from $x_i + \text{Noise}$ to the output (Gupta & Gupta, 2019), as equation (44).

$$\text{Noise} = x_t \cdot (e - e') \tag{43}$$

$$\text{output}_i = f(x_i + \text{Noise}) \tag{44}$$

2) The training data submitted to the follow-up network, which is regarded by the model as the golden rule for self-adjustment, is a kind of difference between the target patient's laboratory results and the laboratory results of one historical patient. The size of this difference is shown in equation (45). At this point, the goal of machine learning model training is to find a stable mapping from $\text{Difference}_i$ to the output, as equation (46). In other words, the model learns to determine whether the historical patient has the disease by the size of the difference between the laboratory results of the historical patient and the target patient. That is, the data point of $x_t \cdot (e' - e)$ becomes the new origin of the whole sample space, $x_t$ becomes the measure of everything, and $(e' - e)$ is the strength of the impact of this measure.

$$\text{Difference}_i = x_i - x_t \cdot (e' - e) \tag{45}$$

$$\text{output}_i = f(\text{Difference}_i) \tag{46}$$

If we were to describe this new neural network structure in a perceptual way, we could say that "something that stays in your mind will someday spring up in your life". Imagine a young man (an untrained model) who decides to study medicine to cure his mother, who is suspected of having an obscure disease (a target patient requiring a customized solution). While learning to treat patients under an experienced doctor (a large training set of data for training), the young man sees many patients and enriches his learning based on the results of the experienced doctor's treatment (update of neural network weights). Unlike other medical students, the young man, while examining each patient, not only considers the patient's lab results but also silently keeps his mother's lab results in mind. He continuously

thinks about the possible cause of the disease and whether his mother is suffering from the same or a similar condition. After a diligent and exhaustive search, he finally returns home with confidence and makes a diagnosis based on his mother's test results, which he knows by heart, and cures her (correctly predicting the diagnosis of the target patient).

### 5.4.3 Validation and Parameter Tuning

A thorough and precise evaluation of a machine learning model's effectiveness is essential for its accurate analysis of novel data. Accurately analyzing new data requires a thorough and precise evaluation of the effectiveness of machine learning models (Doshi-Velez & Kim, 2018). The data in the validation set is not involved in training but serves as a real-world reference to reflect the model's performance on new data that is not involved in training. In order not to waste any of the data collected and to ensure that the model does not overfit on the data already collected, the data is typically used using k-fold cross-validation (Fushiki, 2011).

While this meticulous but inelegant approach makes sense within the context of traditional models, which seek to achieve more accurate answers to general questions outside of the collected data set and rely on averages to describe model performance. This foundational design philosophy, which is less concerned with the accuracy of individual samples, implies that general-purpose models cannot achieve optimal results for each specific problem (Larsen, Hansen, Svarer, & Ohlsson, 1996). However, a machine learning model tailored to an individual patient can take a unique route without the "psychological burden" of not caring about the model's generalization ability because the model will not be used on other patients at all. When the model's generalization ability is no longer paramount in validation set design, the methodology becomes more straightforward. In view of the aim of creating a more trustworthy analysis for the target patient, the validation set is constructed with cases that bear greater resemblance to the target patient, as illustrated in Figure 26. By employing this dataset of similar samples as the validation set to direct the training process of the model, it is feasible to gain a more intuitive understanding of the changes and robustness of the model's loss function throughout the training process, which is intimately tied to the target patients.

The performance of the model for a target patient is rigorously evaluated against a reference standard. This approach not only optimizes the accuracy of the custom model but

also minimizes computational demands via hyperparameter tuning and early training termination. Moreover, the validation set's samples are meticulously selected, mitigating the impact of random factors from the validation criteria to a considerable degree.

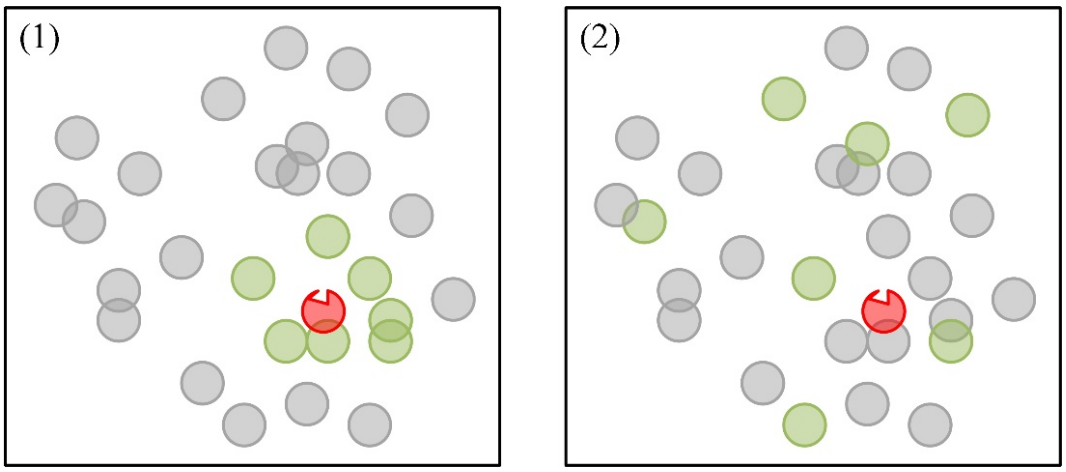



*Figure 26. Different validation set generation methods.*

Note: (1) is a validation set composed of samples (green) that are most similar to the target patient (red, the graph is incomplete because there is no diagnosis result), unlike the traditional randomly generated validation set shown in (2).

**Hyperparameter Optimization**

For custom machine learning models, hyperparameter tuning can be efficiently done using the Optuna framework (Agrawal, 2021; Akiba, Sano, Yanase, Ohta, & Koyama, 2019a) by utilizing parameters that assess model accuracy and stability concerning the chosen target patient. Apart from typical hyperparameters like the number of nodes per layer, epochs, and dropout ratio, optimization of the bias coefficient e is discovered to maintain the accuracy and separability of data in the original sample space, while concurrently improving the model's precision for the designated target patient.

**Early Termination of Training**

The machine learning training process generally involves completing training for a fixed number of epochs or reaching the anticipated value of the loss function. Using a customized validation set, the model is evaluated after each training iteration against this specific data. Training ceases prematurely if the validation set's loss function stagnates or rises notably across successive iterations (Prechelt, 1998, 2012). To achieve optimal model

performance, the final output model preserves the neural network weights with the smallest loss function.

When constructing a validation set with similar sample data, it is crucial to determine the appropriate sample size (Guyon, 1997). Since these most similar samples contain the most relevant information to the target patients, these similar samples must necessarily participate in the training as part of the training set. This means that the data in the validation set and the training set have overlapping parts, and the larger the size of the validation set, the more overlapping parts there are. This will result in the loss function performance of the validation set being closer to that of the training set, which cannot play the role of the validation set as a reference standard. On the other hand, if the number of validation sets is too small, the validation set's loss function may exhibit significant fluctuations throughout training. When we want to analyze the training process and the training results by the trend of the loss function of the validation set, such drastic changes will bring a lot of trouble: For example, the loss function in the early training period has an upward trend because it happens to meet the local optimal solution and ends the training early.

In order to reduce the impact of unreasonable artificially set parameters, a mechanism of a validation set with a dynamic sample size is introduced. Instead of using a fixed number of samples to form the validation set, this mechanism constitutes the validation set based on the number of samples whose similarity satisfies the similarity threshold. Of course, this more flexible validation set can also generate uncertainty because it contains too few similar samples, so the mechanism sets a minimum number of samples for the validation set.

This dynamic threshold can ensure the stability of the validation set's performance throughout the early stages of the large-scale screening project's initiation, when the amount of data accumulated is small. It also ensures that the validation set does not lose its difference from the training set as more samples are added and the amount of data becomes larger. Note: The samples selected in the validation set must be the real samples before oversampling, and cannot contain the virtual samples created by oversampling.

## 5.5 Experiments

To validate the conjecture in the hypothesis, it is imperative during the experimental phase to concurrently focus on the model's predictive capability and the quantity of parameters. Enhancing model accuracy by merely increasing the number of parameters would fail to justify the significance of customization. The study will conduct two phases of experiments. The first phase aims to perform functional verification experiments on the proposed approaches and models. This phase will validate the efficacy of the custom model and compare its performance with other commonly used models based on specific evaluation criteria. The second phase will focus on the state-of-the-art comparison experiment to demonstrate the optimal performance levels of the custom model by optimizing specific hyperparameters. And keep in mind the particular requirements of the scenario during the experiment to ensure that multiple objectives are balanced rather than simply refreshing the best performance of a particular metric. The experiments were conducted using a workstation equipped with high-performance hardware, including an Intel Core i7-12700K CPU, an RTX3090ti GPU with 24 GB of video memory, 32 GiB DDR4 RAM, and an SSD for secondary storage. The experiments were performed multiple times to ensure reliability, and the average results were recorded for analysis.

### 5.5.1 Functional Verification

In the 5.4 Specific Solutions section, three separate levels of custom machine learning algorithm research are presented: Data Augmentation with Focus, Neural Networks with Attention, and No Longer Random Criteria. The approaches presented in each of these three levels can be summarized as: Targeted data augmentation (TDA), Adaptive attention intensity (AAI), and Relevant validation sets (RVS). In this section, the effectiveness of the TDA, AAI, and RVS are verified separately and in combination. Furthermore, for each combination of approaches, the experiments were repeated several times to show their average levels finally. Fifty custom models were built and trained to make outcome predictions for 50 automatically generated the selected target problem with a fixed training set. The performance of the regression models is evaluated by Mean Absolute Error (MAE), Root Mean Square Error (RMSE), and R-square metrics.

**Data Set Construction**

Real-world data always have more or fewer flaws, such as missing data, some data being incorrectly recorded, etc. When these data that need to be cleaned or feature-engineered are used, the comparison of accuracy between models is easily influenced by the data themselves, which is not conducive to simply comparing the strengths and weaknesses of the models themselves. Therefore, an essentially uniform and stable sample space is created by random number generation. This has the added benefit of having the freedom to control the size of the training set, allowing exploration of the performance of custom models at different scales.

In constructing the training set, the essential computational relationships in the real world are combined to derive an "artificial formula" as a correspondence between input and output. The formula is sufficiently complex, and different variables do not have the same magnitude of influence on the overall output, which can better simulate the relationship between multiple inputs and outputs in the real world. A total of 10 independent variables and one dependent variable were set, and the rules for generating random numbers are shown in Equation 47. Three training sets of 500, 1000, and 2000 were constructed, corresponding to different densities of the sample space, respectively.

$$x_9 * (\ln x_2 + x_3) + \sqrt{x_4/(x_5 + x_6)} * \sin x_7 + {x_8}^2/(x_1 + x_{10}) \quad (47)$$

where $x_1 \in \text{randint}(101, 200)$, $x_2 \in \text{randint}(30,100)$, $x_3 \in \text{randint}(1, 7)$, $x_4 \in \text{uniform}(1, 10)$, $x_5 \in \text{uniform}(1, 10)$, $x_6 \in \text{uniform}(1, 10)$, $x_7 \in \text{randint}(-\pi, \pi)$, $x_8 \in \text{randint}(1, 100)$, $x_9 \in \text{randint}(-100, 100)$, $x_{10} \in \text{randint}(-100, 0)$.

**Baseline and Data Preprocessing**

The most basic back propagation neural network model (Murtagh, 1991) with three sequential fully connected layers is chosen as the baseline for comparison, and this model is widely used at the end of various complex models. AAI is the only approach that involves the change of model structure, and it only adds one single-parameter fully connected layer to ensure the uniformity of model complexity. The original train and validation sets are randomly divided according to the ratio of 0.1. In the pre-processing session of the

experimental data, only the data set is normalized without any additional feature engineering, or data cleaning means.

**Model Construction**

Based on the number of independent variables, the number of nodes in each of the three fully connected layers was set to 100, and each layer was output using the activation function ReLU. The final output layer has only one node and does not use an activation function. The whole neural network contains 21,402 trainable parameters. The Adam (Adaptive Moment Estimation (Kingma & Ba, 2014)) and mean absolute percentage error were chosen as the optimizer and loss function . The overall model construction was simplified as much as possible to evaluate the merit of the final output without using complex techniques. Callbacks were used for the model, *val_loss* was used as the monitored quantity, and the optimal model is saved. The batch size was chosen to be 256, and the maximum epochs were 500.

**Parameters of the Improvement Approaches**

The parameters of the improvement approaches were chosen using invariant parameter settings to verify the generalizability of the improvement scheme. The following is a description of the special parameters.

**Similarity threshold**: In this experiment phase, the similarity threshold was set to a fixed value of 2.5. **Augmentation threshold**: In this experiment phase, the proportion of the oversampled minority class was set at a fixed value of 0.3. **The number of results identified as similar:** In this stage, this parameter is set to a fixed number of 10, i.e., the ten samples that are most similar to the selected target problem are selected as the validation set. **Bias coefficient(e)**: as introduced in 3.2 above. In this phase, the bias coefficient is set to a fixed value of -0.2.

**Experimental results and analysis**

The experimental results are shown in Tables 13, 14, and 15, where the T, R, and A are short for TDA, RVS, and AAI. More visual statistics are shown in Figure 27 where the data are consistent with Tables 13, 14, and 15.

Table 13. The mean absolute errors when different combination approaches were applied to various data sets

| SIZE | BASELINE | TDA | RVS | AAI | TDA+RVS | TDA+AAI | RVS+AAI | T+R+A |
|---|---|---|---|---|---|---|---|---|
| 500 | 199.01±3.64 | 138.57±22.03 | 103.85±3.47 | 160.75±21.86 | 68.92±4.63 | 97.36±6.8 | 87.3±9.33 | 51.38±0.72 |
| 1000 | 121.11±12.43 | 84.5±17.06 | 69.9±3.39 | 108.51±16.75 | 47.55±6.02 | 39.52±3.42 | 41.47±5.6 | 27.89±1.09 |
| 2000 | 59.49±11.91 | 31.93±2.63 | 39.71±1.07 | 43.08±6.07 | 27.91±1.79 | 29.75±1.08 | 38.69±0.83 | 26.81±0.89 |

Table 14. The root mean squared error when different combination approaches were applied to various data sets

| SIZE | BASELINE | TDA | RVS | AAI | TDA+RVS | TDA+AAI | RVS+AAI | T+R+A |
|---|---|---|---|---|---|---|---|---|
| 500 | 296.93±4.8 | 226.15±14.27 | 142.34±5.11 | 249.01±27.88 | 100.38±16.59 | 159.1±7.82 | 127.25±18.99 | 67.52±3.62 |
| 1000 | 198.66±10.61 | 167.9±33.22 | 130.29±5.87 | 182.1±12.14 | 91.48±3.75 | 72.79±14.1 | 64.68±9.61 | 48.98±4.23 |
| 2000 | 121.76±25.02 | 63.34±2.7 | 67.85±2.47 | 87.34±18.67 | 63.78±3.61 | 62.85±1.46 | 66.44±1.32 | 58.73±1.06 |

Table 15. The R-square when different combination approaches were applied to various data sets.

| SIZE | BASELINE | TDA | RVS | AAI | TDA+RVS | TDA+AAI | RVS+AAI | T+R+A |
|---|---|---|---|---|---|---|---|---|
| 500 | 0.5336±0.0152 | 0.7285±0.0334 | 0.8927±0.0076 | 0.668±0.0709 | 0.9556±0.0036 | 0.8658±0.0131 | 0.9124±0.0244 | 0.9758±0.0026 |
| 1000 | 0.7831±0.0233 | 0.8395±0.0643 | 0.9068±0.0085 | 0.8175±0.0246 | 0.9432±0.0172 | 0.9698±0.0113 | 0.9765±0.0071 | 0.9871±0.0024 |
| 2000 | 0.9366±0.0268 | 0.976±0.009 | 0.9811±0.0014 | 0.9643±0.0153 | 0.9832±0.0018 | 0.9814±0.0020 | 0.9818±0.0007 | 0.9874±0.0016 |

Table 16. Comparison of baseline and custom models after simplification of the number of model parameters.

| SIZE | MAE BASELINE | MAE T+R+A | RMSE BASELINE | RMSE T+R+A | R-SQUARE BASELINE | R-SQUARE T+R+A |
|---|---|---|---|---|---|---|
| 500 | 311.99±8.60 | 106.51±9.59 | 392.90±16.36 | 160.46±11.67 | 0.1822±0.0684 | 0.8631±0.0203 |
| 1000 | 262.32±19.31 | 78.32±7.59 | 344.85±31.26 | 132.19±19.35 | 0.4506±0.0010 | 0.9182±0.0234 |
| 2000 | 151.72±6.54 | 37.60±1.70 | 221.39±18.63 | 69.47±3.14 | 0.7977±0.0348 | 0.9801±0.0018 |

Note: With a model of 20 nodes per layer, the number of parameters drops to 1082. the custom model can still have a better play.

By observing the performance of the custom models on the training sets at the scales of 500, 1000, and 2000, the following conclusions can be drawn. (1) The three approaches introduced, the TDA, AAI, and RVS, can effectively improve the accuracy of prediction results under various scales individually. Both MAE and RMSE decreased, and R-square steadily increased. (2) Combining two or three approaches can achieve further improvement. (3) It also appears that the superimposed effect of the two approaches is not as good as that of the single approach, indicating that the relevant parameters need further adjustment. (4) In the case of a small amount of data, the baseline performance varies greatly among the different selected target problem samples. Still, if the three improved approaches are used simultaneously, the accuracy of each selected target problem prediction can be controlled within an acceptable range.

In order to verify the performance of the model under different requirements, the model with a smaller number of parameters is used to show the effect under lightweight requirements. Experiments with fewer nodes and fewer parameters (the number of parameters is reduced to 1/20 of the original) are shown in Table 16.

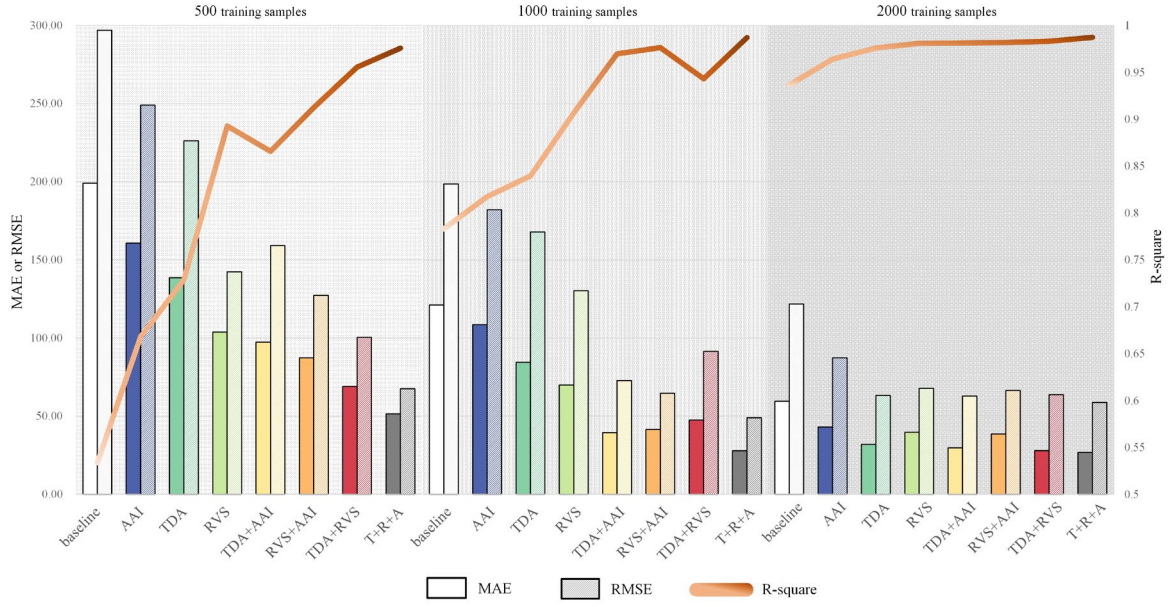



*Figure 27. Statistics of experimental results in the functional verification stage.*

It is easy to understand that TDA can have improvement on the selected target problem, and the other two approaches will be additionally further validated. The

effectiveness of these schemes can be verified by the trend of loss changes during the training process. In order to better demonstrate the actual effect brought by AAI and RVS during the training process, this chapter recorded the change process of the loss function in different settings. In several experiments, different approaches were chosen for the same target problem for repeated training, and the results were recorded.

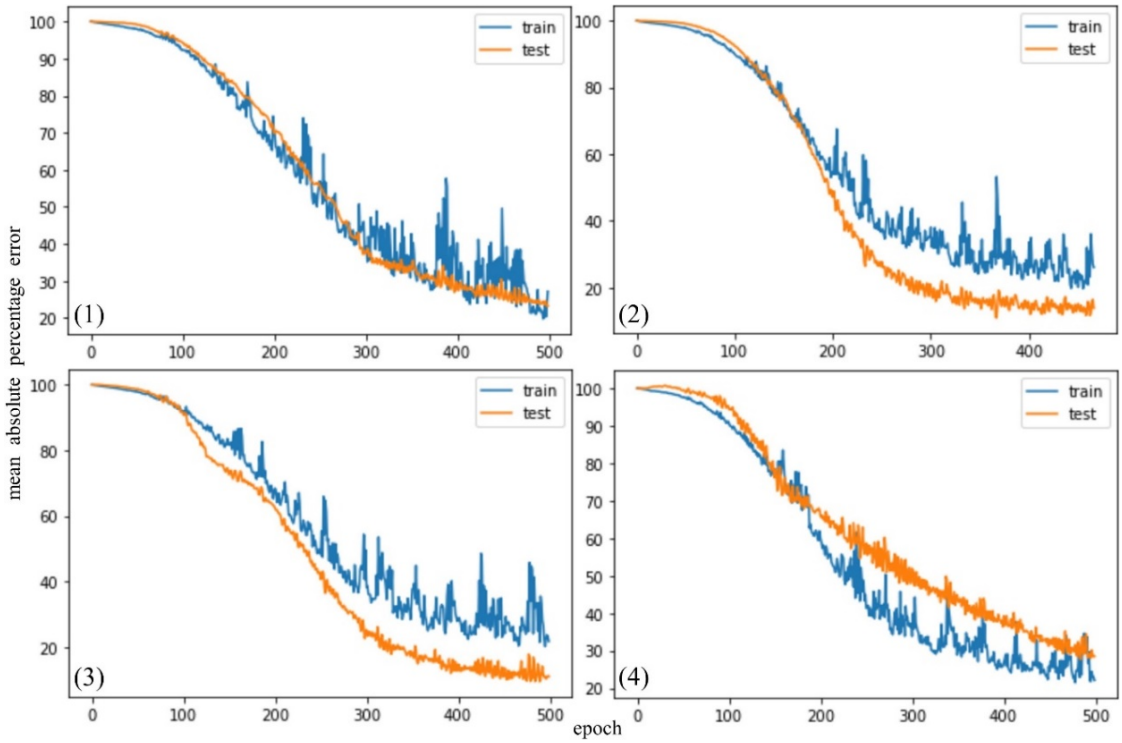



*Figure 28. The loss and val_loss during training.*

Note: (1) baseline; (2) when RVS approach is called (the correct answer is used as the validation set), and the AAI approach is called; (3) when RVS approach is called (the ten most similar solutions are used as the validation set), and the AAI approach is called; (4) when RVS approach is called (the ten least similar solutions are used as the validation set), and the AAI approach is called.

Figure 28(1) shows the trend of loss of baseline. It can be seen that the validation set randomly divided by a ratio of 0.1 is more consistent with the decreasing trend of the loss of the training set.

Figure 28(2) shows the loss trend when the correct answer is used in the validation set, and the AAI approach is called. At this point the validation set has only one sample,

the input to the validation set is $x_q$ (x-question) of the selected target problems, and the answer to the validation set is the true y of the selected target problems. The validation set loss is calculated by subtracting y from $y_{predict}$, which is derived from the model prediction based on $x_q$. Note that the y-value of the validation set called here is the accurate result of the selected target problem calculated directly by the formula. Usually, only $x_q$ of the selected target problem can be obtained, and $y_{value}$ calculated by the selected target problem should not be used. Here is a special call to observe the actual trend of the model training process for the accuracy of the selected target problem. It can be found that the model's accuracy for the selected target problem is consistently better than that for the overall training set when the bias approach is called.

Figure 28(3) shows that the AAI approach is called when the ten most similar solutions are used as the validation set. Here, it can be seen that the decreasing trend of *val_loss* is very similar to the actual trend in Figure 28(2). This indicates that using the ten most similar solutions as the validation set is a good representation of the movement of the model's accuracy for the selected target problem during the training process.

Figure 28(4) shows that the bias approach is called, and the ten least similar solutions are used as the validation set. It can be seen that the prediction accuracy of models for the ten least similar to the selected target problem samples is consistently lower than the accuracy of the overall training set. The reverse proves the preference of the custom model for the selected target problem. This, inversely, substantiates the hypothesis.

After the above analysis of the experimental results, the effectiveness of the proposed three improvement approaches can be demonstrated. It is also verified that the custom model is much more adaptable than the traditional model in different requirement situations. This phase uses a very straightforward approach to reduce the number of model parameters in the form of lowering the number of nodes per network layer of the model, which at the same time can significantly reduce the training time

of the model and the inference time after deployment. In this case, the accuracy of the traditional model decreases substantially to an unacceptable level after the number of model parameters is greatly reduced. The custom model, on the other hand, can guide the loss function of the model during training according to the actual accuracy of the scenario requirements, which greatly ensures its own accuracy and reflects its strong robustness.

### 5.5.2 Custom Model Performance

It is time to show how custom models perform on heart disease datasets. The overall program running logic for this phase is to train a unique custom model for each patient and make predictions. For each patient, the data for this patient is cut out of the original dataset and all the data left in the dataset is used as the initial training set. The patient's diagnosis in this separate data sample is then removed to serve as the test set (the target problem). After that, the data processing, model training, and parameter tuning are performed guided by Data Augmentation with Focus, Neural Networks with Attention, and No Longer Random Criteria, respectively. A custom model is trained and predictions are made for this patient.

In this study on machine learning, the backbone network used is a basic backpropagation neural network model with three sequential fully connected layers. The number of nodes in each of the three fully connected layers is set to 130 based on the number of independent variables, with each layer output using the ReLU activation function. The final output layer consists of a single node and uses the sigmoid activation function. The model comprises 36,012 trainable parameters and employs the Adam optimizer and binary_crossentropy loss function.

At this point, after the input data has been run through the entire model, the output will be a number in the interval 0 to 1. The meaning of this number is the probability of having a heart disease, and this chapter classifies individuals with data greater than 0.5 as patients. This multilayer neural network also known as MLP is a constructed classifier.

To evaluate the model's efficacy, its construction is simplified, and callbacks are

employed to monitor and save the optimal model based on the monitored validation loss. The batch size is set to 256, and the maximum epochs are set to 200. The bias coefficient and drop-out ratio are selected for each target patient using the Optuna framework, which repeats experiments with multiple parameters and outputs the optimal parameter based on the monitored binary_crossentropy of the validation set. The variation interval for the bias coefficient is -0.5 to 0.5, and for the drop-out ratio, it is 0 to 0.3. The results of the optimal parameters: similarity threshold: 3.8, Number of results identified as similar: 15, and augmentation threshold: 0.5. To compare the model with other competing models, 20% of the data from the Cleveland dataset is set aside as a test set consisting of 25 patients and 35 healthy individuals to be distinguished. The custom model is constructed and classified for each selected target patient in turn using Algorithm 4, and the final results are presented in Table 17.

Table 17. Confusion Matrix of Custom Model.

| actual \ predict | Heart = 1 | Heart = 0 |
|---|---|---|
| Heart = 1 | 24 | 1 |
| Heart = 0 | 2 | 33 |

Note: Accuracy = 0.9500, Recall = 0.9600, Precision = 0.9231, f1-Score = 0.9412, MCC=0.8982

The entire process is repeated for each patient, as described in Algorithm 2 in appendix.

The entire Cleveland dataset is iterated in order to better verify the applicability of the method. For the whole dataset, each sample is treated as the selected target patient, and the custom model is constructed and classified for each selected target patient in turn, and the final results are shown in Table 18.

Table 18. Confusion Matrix of Custom Model.

| actual \ predict | Heart = 1 | Heart = 0 |
|---|---|---|
| Heart = 1 | 131 | 6 |
| Heart = 0 | 8 | 152 |

Note: Accuracy = 0.9529, Recall = 0.9562, Precision = 0.9424, f1-Score = 0.9493, MCC=0.9053

Similarly, the custom model achieves better results on the UCI dataset because of the richer amount of data, and the results are shown in Table 19.

Table 19. Confusion Matrix of Custom Model.

| actual \ predict | Heart = 1 | Heart = 0 |
|---|---|---|
| Heart = 1 | 345 | 11 |
| Heart = 0 | 13 | 377 |

Note: Accuracy = 0.9678, Recall = 0.9691, Precision = 0.9637, f1-Score = 0.9664, MCC=0.9356

## 5.6 Comparative Analysis

### 5.6.1 Comparison with the work of others

In experiments utilizing artificial simulation data, each of the three methods employed by the custom model—both individually and in combination—demonstrated a notable improvement over the traditional MLP model. Furthermore, they exhibited robust performance even under lightweight constraints. In simulating a large-scale screening of the heart disease dataset, an accurate model was built (96.8% accuracy) without introducing additional information and without any relevant medical background. If all patients labeled as rare were examined in further detail, more patients would be distinguished, and the accuracy and recall would be improved. But this achievement cannot be credited to the custom model because the model still cannot solve the problem caused by insufficient data out of nothing.

The comparison with other outcome solutions for the same dataset is detailed in Table 20 (Amin et al., 2019; Djerioui, Brik, Ladjal, & Attallah, 2019a; El-Bialy, Salamay, Karam, & Khalifa, 2015; Latha & Jeeva, 2019; Paul et al., 2016; Raihan et al., 2019; Subanya & Rajalaxmi, 2014; Waqar et al., 2021) and far exceeds some solutions with medical backgrounds. In large-scale screening involving millions of people, each percentage point increase in accuracy and recall may save 10,000 more families.

Table 20. Comparison of Experimental Results.

| Source | Technique used | Matrices used for evaluation (%) | | | |
|---|---|---|---|---|---|
| | | Accuracy | Precision | Recall | Fl-measure |
| (Amin et al., 2019) | Vote | 87.41 | 79.41 | | 78.10 |
| (Latha & Jeeva, 2019) | Ensemble learning | 85.48 | | | |
| (Raihan et al., 2019) | Artificial neural network | 84.47 | 79.97 | 82 | 85.17 |
| (Paul et al., 2016) | Neural network with fuzzy logic | 80 | | | |
| (El-Bialy et al., 2015) | Decision tree | 78.54 | | | |
| (Subanya & Rajalaxmi, 2014) | SVM | 86.76 | | | |
| (Djerioui, Brik, Ladjal, & Attallah, 2019b) | Neighborhood component analysis and SVM | 85.43 | | | |
| (Waqar et al., 2021) | SMOTE based artificial neural network | 96.1 | 95.7 | 95.7 | 96 |
| **Proposed work** | **custom model** | **96.8** | **96.4** | **96.9** | **96.6** |

For this case study, the analysis time is approximately 1 minute per patient, aligning with the time requirements for large-scale disease screening. As the dataset expands to the order of magnitude of 10,000, the time to retrain and diagnose for each patient rises to 5 minutes. Since only data selected by physicians are included in the dataset and most of them are similar. So 10,000 data can already very adequately include common patients as well as rare patient conditions. Because the slowest process in implementing large-scale screening is the somewhat tedious process of ECG testing, the computational process of machine learning does not slow down the entire screening process. The equipment requirements involved in the training and analysis of the model are very common and easy to implement, and the accuracy can be improved by adding some hyperparameters for optimization or improving the number of trials as needed; or the analysis time per patient can be shortened at the expense of a little accuracy, reducing the cost of computing equipment. This suggests that we can identify a significant number of heart patients or

potential patients in the population without resorting to costly and invasive tests, offering a potent tool for life-saving interventions.

This innovative custom model also has some more far-reaching implications. 1. This approach, which involves developing a tailored model for each patient considering their unique differences, makes the testing process more palatable to the individual. This form of testing is more comfortable for patients, both from an ethical standpoint and from a personal privacy standpoint. 2. Clinical-related systems cannot rely solely on old patient data, so models must be continually adapted and developed based on new patient data in order for the system to function smoothly and correctly. But, for traditional general-purpose models, the idea of collecting data and then training a unified model does not allow for real-time data updates. Custom algorithms offer a solution, as each patient's training dataset is distinct, allowing for the most up-to-date information. When any patient is accurately diagnosed after a thorough examination and expert consultation, the data of such a patient can immediately become part of the training set database, as long as the patient is willing to contribute his or her own data. 3. Trustworthy interpretation is vital for ML algorithms, especially when the model's outputs relate directly to an individual's health. Without adequate model interpretation, it is dangerous to use these applications in a clinical setting. Although the process of building the machine learning involved in this study still does not provide a complete picture of all the operational details in the entire black box, the more cautiously designed ablation experiments argue to a large extent for the push up in accuracy that comes from customization of the model.

### 5.6.2 Comparison with the work of the previous chapter

Because the framework of the algorithm used in this chapter is obtained by adding new mechanisms to Chapter Four. Therefore, the algorithms in Chapter Four are applied to the scenarios in this chapter for experiments to test the effectiveness of the newly added mechanisms in this chapter. The results achieved by the algorithm of Chapter Four on the UCI dataset are shown in Table 21.

Table 21. Confusion Matrix of Custom Model without consideration of scenario-specific requirements.

| actual \ predict | Heart = 1 | Heart = 0 |
|---|---|---|
| Heart = 1 | 338 | 18 |
| Heart = 0 | 16 | 374 |

Note: $\text{Accuracy} = 0.9544$, $\text{Recall} = 0.9494$, $\text{Precision} = 0.9548$, $\text{f1-Score} = 0.9521$, $\text{MCC}=0.9086$

It can be seen that the performance of the customised model decreases without the use of the dynamic thresholding, data updating and other mechanisms proposed in this chapter. In addition to the difference in accuracy, the newly added mechanisms in this chapter can also bring about an improvement in overall efficiency. This just shows that it is very important to deeply understand and incorporate the actual requirements of the scenario into the design process of the algorithm.

### 5.6.3 Limitations

Despite the advantages of the customized solution, its limitations cannot be overlooked. While traditional general-purpose models can diagnose all new patients after completing training, customized algorithms require a separate model to be trained for each new patient.

Suppose the training dataset has $s$ training samples, $f$ features(dimensions), and the model has $h$ hidden layers, each containing $n$ neurons. Given that this is a binary classification problem, there is only one output neuron. And $i$ is the number of iterations. Under the MLP framework used in this study, the time complexity of training a model and the time complexity of the model to complete one diagnosis are respectively:

$$O_{\text{trian}}(s \cdot f \cdot n^h \cdot i) \tag{48}$$

$$O_{\text{diagnosis}}(f \cdot n^h) \tag{49}$$

Therefore, when analyzing data of $m$ patients, the time complexity for the traditional approach is:

$$O_{\text{trian}}(s \cdot f \cdot n^h \cdot i) + O_{\text{diagnosis}}(m \cdot f \cdot n^h) = O(m \cdot f \cdot n^h) \tag{50}$$

For the customized approach addressing these $m$ patients, the time complexity is:

$$O_{custom}\left(m \cdot f \cdot n^h(s \cdot i + 1)\right) = O\left(m \cdot f \cdot n^h \cdot s \cdot i\right) \quad (51)$$

As the value of $m$ increases, the disparity in time between the two approaches widens. Fortunately, these calculations can be distributed across devices or expedited using modern computational tools. Overall, the time taken by the customized solution for both training and diagnosis is inconsequential compared to the duration of even a minor procedure in a medical examination.

Future research should explore providing custom models for patients through migration techniques instead of starting from scratch.

## 5.7 Validation of the Specific Requirement of Large-Scale Disease Screening

The approach outlined in the chapter meticulously addresses the unique requirements of large-scale disease screening, demonstrating a profound departure from traditional methodologies. This analysis explores how the chapter's approach aligns with the specified needs of large-scale screening and why traditional models fall short, with a focus on the experimental evidence provided in section 5.5.

**Efficiency and Scalability**

Approaches proposed in this chapter. The adoption of machine learning models tailored for specific scenarios, as described in the chapter, facilitates the efficient handling and analysis of large datasets characteristic of wide-scale screenings. The custom models, through focused data augmentation and attention mechanisms, optimize computational resources by prioritizing relevant data, thereby enhancing scalability and efficiency.

Traditional shortcomings. Traditional models often prioritize generalizability over specificity, leading to inefficiencies when applied to large-scale datasets. They tend to require extensive computational resources for training on broad datasets, lacking the focused approach that can streamline processing for specific screening contexts.

**Scenario-based models can outperform traditional general-purpose models with**

**$\frac{1}{4}$ the training set data, or $\frac{1}{20}$ the number of model parameters.**

**Accuracy and Sensitivity**

Approaches proposed in this chapter. The custom machine learning models are specifically designed to enhance accuracy and sensitivity, crucial for disease screening. By incorporating individual patient data and employing targeted data augmentation, these models ensure that the unique characteristics of each case are considered, improving the precision of screening outcomes.

Traditional shortcomings. General-purpose models may not achieve the same level of accuracy and sensitivity due to their broad focus. These models are trained to perform well across a wide range of scenarios, which can dilute their effectiveness in specific screening contexts, potentially leading to higher rates of false negatives or positives.

**Scenario-based models outperform traditional universal models by up to 10% in accuracy, recall, precision, F1-measure, and other indicators.**

**Adaptability and Customization**

Approaches proposed in this chapter. The chapter emphasizes the importance of adaptability and customization, with machine learning models tailored to the nuanced demands of specific screening scenarios. This bespoke approach allows for the integration of new data and adjustment to emerging disease patterns, ensuring that the models remain relevant and effective over time.

Traditional shortcomings. Traditional models lack this level of adaptability and customization. Once developed, these models might not easily incorporate new data or adjust to changing disease dynamics, making them less effective as screening tools over time.

**Ethical Considerations and Data Privacy**

Approaches proposed in this chapter. The tailored approach inherently considers ethical and data privacy concerns by ensuring that individual patient data is used

responsibly and securely. The customization process allows for adherence to strict data protection regulations, safeguarding patient information throughout the screening process. Due to the super lightweight design, in large-scale screening programs, it is permissible for individuals to conduct offline checks on their personal devices based on their information. This ensures the protection of personal information from being disclosed.

Traditional shortcomings. Traditional models, with their broad application focus, might not adequately address specific ethical and privacy concerns associated with large-scale screenings. The lack of customization can lead to challenges in ensuring data privacy and ethical use of information.

**Interdisciplinary Integration**

Approaches proposed in this chapter. By leveraging scenario-specific data and integrating interdisciplinary knowledge, the chapter's approach fosters a more collaborative framework between machine learning and domain experts. Because the health care provider can adjust the composition of the training set at any time, it can provide more thoughtful testing for subsequent inspectors. This ensures that the developed models are both technically sound and clinically relevant, enhancing the overall effectiveness of disease screenings.

Traditional shortcomings. Traditional models often operate in silos, with limited input from domain experts outside of the machine learning field. This can result in models that, while technically proficient, may lack the clinical relevance and practical applicability needed for effective disease screening.

The experimental section of the 5.5 further substantiates the superiority of the chapter's approach over traditional methodologies in meeting the specific requirements of large-scale disease screening. Through targeted customization, ethical consideration, and interdisciplinary collaboration, these machine learning models demonstrate enhanced efficiency, accuracy, and adaptability, directly addressing the unique challenges of large-scale disease screening contexts.

## 5.8 Proof of the Principle

The efficacy of the approaches proposed in the chapter—specifically Targeted Data Augmentation (TDA), Adaptive Attention Mechanism (AAI), and Relevant Validation Sets (RVS)—can be understood and validated through a blend of concepts from information theory and statistical learning. These approaches tailor machine learning models to individual patients or scenarios, focusing on enhancing the specificity and sensitivity of the models for particular applications. Here, we'll explore the mathematical basis that supports why these methodologies are effective, particularly in the context of disease screening models.

### 5.8.1 Targeted Data Augmentation (TDA)

Data augmentation is a technique to artificially increase the size and diversity of the training dataset by generating new data points from the existing ones. In the context of TDA, the aim is to focus on generating data points that are similar to the target patient or scenario, thus making the model more sensitive to the specific characteristics of the target.

From an information theory perspective (Graham, Drake, Djorgovski, Mahabal, & Donalek, 2013; Porta et al., 1999; Rosenberg & Hirschberg, 2007), the entropy $H(X)$ of a dataset $X$, which measures the amount of information contained in $X$, should be considered. Augmenting data specifically tailored to resemble the target patient can be seen as reducing the entropy of the dataset $X$ with respect to the target patient's data distribution $P_t$, effectively increasing the mutual information $I(X; P_t)$ between $X$ and $P_t$. This increase in mutual information means the augmented dataset contains more information relevant to the target, improving the model's ability to learn features specific to the target's data distribution.

Mathematically, the mutual information is defined as:

$$I(X; P_t) = H(X) - H(X|P_t) \tag{52}$$

where $H(X|P_t)$ is the conditional entropy of $X$ given $P_t$. By focusing the augmentation process on the target $P_t$, we aim to minimize $H(X|P_t)$, thus maximizing $I(X; P_t)$ and

making the model more effective for the target patient.

Traditional data augmentation indiscriminately increases the diversity and size of the dataset without specific regard to the target scenario's characteristics. Let $X$ be the dataset and $P_t$ the target patient's data distribution. In traditional augmentation, the aim is simply to increase $H(X)$, the entropy or the amount of information contained in X, without ensuring that this information is relevant to $P_t$.

The advantage of TDA is its focus on increasing $I(X; P_t)$, the mutual information between X and $P_t$, rather than just $H(X)$. By maximizing $I(X; P_t)$, TDA ensures that the augmented data contains information that is more relevant and specific to the target, leading to a model that is better tuned to the specific requirements of the scenario.

### 5.8.2 Adaptive Attention Mechanism (AAI)

The adaptive attention mechanism focuses on selectively prioritizing features relevant to the target patient during the learning process. This can be understood through the lens of a noise channel in information theory, where the goal is to transmit information with minimal loss.

Consider a neural network as a complex communication channel where the input data X is transmitted through the network to produce an output Y. The presence of irrelevant features or data can be considered as noise in this channel, which may obscure the signal (relevant features). By implementing an attention mechanism that adaptively weights features based on their relevance to the target, this chapter effectively increases the channel capacity $C$, which is the maximum rate at which information can be reliably transmitted over the channel (W. C. Lee, 1990; Verdú, 1990, 1994).

The channel capacity $C$ is related to the mutual information between the input and output of the channel:

$$C = \max_{P(X)} I(X; Y) \tag{53}$$

By maximizing the mutual information $I(X; Y)$ specifically for features relevant to the target, the AAI mechanism ensures that the neural network channel more efficiently

transmits information pertinent to making accurate predictions for the target patient.

In traditional learning mechanisms, all features are treated equally, which can lead to models that are not optimally sensitive to the specific features that are most informative for the target scenario. This can be seen as a communication channel with a certain capacity $C$, where the goal is to transmit the signal (relevant information) through noise (irrelevant information).

The capacity of this channel, given by the Shannon-Hartley theorem, is:

$$C = B \log_2 \left(1 + \frac{S}{N}\right) \tag{54}$$

where $B$ is the bandwidth (in this context, the complexity or capacity of the model to learn), $S$ is the power of the signal (relevant information), and $N$ is the power of the noise (irrelevant information).

AAI focuses on increasing $S/N$, the signal-to-noise ratio, by giving more weight to features relevant to the target scenario. This effectively increases $C$, the capacity of the model to learn relevant information, leading to a more accurate and specific model for the scenario.

### 5.8.3 Relevant Validation Sets (RVS)

The concept of using validation sets most similar to the target patient ensures that the model's performance is evaluated on data that is most representative of the target's distribution. From an information theory standpoint, this approach ensures that the entropy of the validation set $H(V)$ is closely aligned with the entropy of the target patient's data distribution $H(P_t)$.

By minimizing the Kullback-Leibler divergence $D_{KL}(P_t|V)$ between the target distribution $P_t$ and the validation set distribution $V$, this chapter ensures that the validation process provides a more accurate measure of the model's ability to predict outcomes for the target patient:

$$D_{KL}(P_t|V) = \sum_{x \in P_t} P_t(x) \log \frac{P_t(x)}{V(x)} \tag{55}$$

A lower $D_{KL}$ indicates that the validation set is more representative of the target distribution, leading to more reliable estimates of model performance for the specific target scenario.

Traditional validation methods use randomly selected subsets of data, which may not represent the specific distribution of the target scenario, leading to less reliable estimates of model performance. Let $V$ represent the validation set, and $P_t$ the target patient's data distribution. The aim is to minimize the divergence $D_{KL}(P_t|V)$ between $P_t$ and $V$.

RVS specifically selects $V$ to be more representative of $P_t$, effectively reducing $D_{KL}(P_t|V)$ and ensuring that the validation process gives a more accurate and relevant measure of the model's performance in the specific scenario.

Through the lens of information theory and statistical learning, the approaches of TDA, AAI, and RVS are designed to enhance the mutual information between the model inputs and outputs relevant to the target scenario, reduce noise and maximize the throughput of relevant information, and ensure that model evaluation is closely aligned with the target's characteristics. These mechanisms collectively enhance the model's ability to learn and predict with high specificity and sensitivity, making them particularly effective for applications like disease screening where precision is paramount.

## 5.9 Summary

This chapter has undertaken a rigorous examination of machine learning paradigms, with a particular focus on the customization of models to meet the unique demands of specific application contexts. By adopting a scenario-specific approach, particularly in the domain of large-scale heart disease screening, this chapter have illustrated the substantial enhancements in model accuracy and efficiency that can be achieved. This methodological innovation, underpinned by targeted data augmentation, the integration of attention mechanisms, and the application of non-arbitrary selection criteria, establishes a new precedent for the deployment of machine learning in critical healthcare applications.

**Innovations and Contributions**

The research addressed the inherent limitations of generalized models, such as suboptimal resource utilization and a lack of interdisciplinary integration, through the development of models that leverage scenario-specific data. This approach ensures heightened accuracy and relevance in applications. And it proves the effectiveness of customization both positively and negatively through experiments. Furthermore, this chapter explored the ethical and practical ramifications of these models in healthcare, highlighting their potential to foster personalized patient care while maintaining data privacy and security.

The architecture presented in this chapter is developed from the one presented in the previous chapter. It is reflected in the specific operation flow by adding new tasks and new settings to the original flow. The flowchart of the algorithm applied to large-scale heart disease screening proposed in this chapter is shown in Figure 29. The grey part is the flow consistent with the previous chapter, and the blue part is the new tasks added on the basis of the previous chapter.

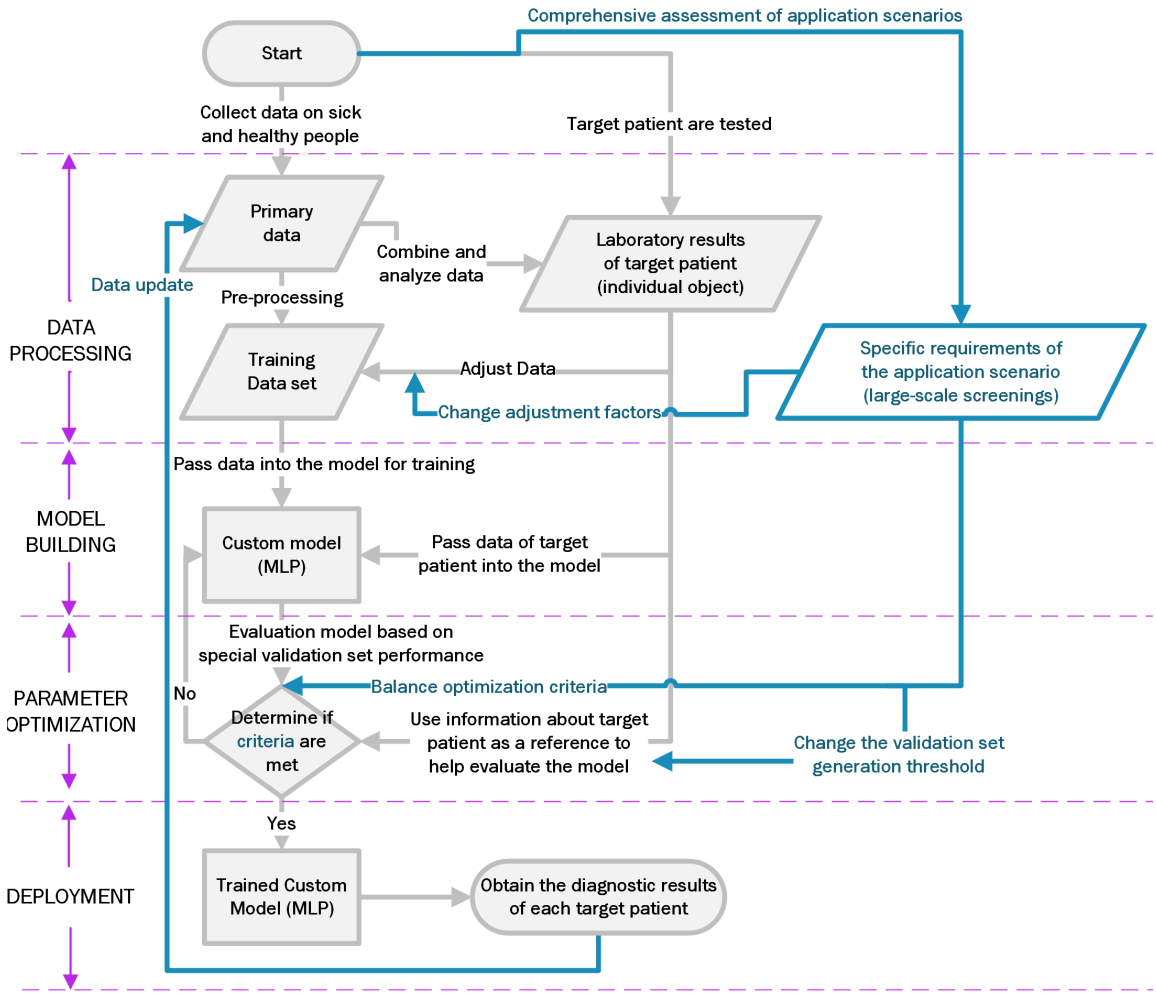



*Figure 29. Flowchart for meeting scenario (large-scale heart disease screening) specific requirements.*

**Addressing Core Challenges**

Efficiency and Accessibility. The methodology enhances computational resource efficiency, enabling the deployment of advanced machine learning models in resource-limited settings. This optimization is crucial for broadening the accessibility and real-world applicability of these technologies. Experiments demonstrate that even when the number of parameters is reduced to one-twentieth of the original, the customized scheme still shows excellent accuracy, far exceeding that of the general-purpose model. This efficiency opens up the possibility of updating and using data in real-time.

Interdisciplinary Integration. Because of the large-scale testing, experts and doctors can readily add data to the training set that is typical of what is newly discovered in testing.

By embedding domain-specific knowledge into the model development process, this chapter facilitates a collaborative framework that bridges the gap between machine learning experts and domain specialists, enriching the model's utility and efficacy.

**Future Directions**

Looking ahead, this chapter opens numerous research avenues, notably in the realms of transfer learning for model generalization, further integration of interdisciplinary knowledge, and the development of strategies for computational optimization. These directions promise to enhance the scalability, performance, and resource efficiency of machine learning models tailored to specific scenarios.

In summary, the methodologies and insights detailed herein mark a significant advancement in machine learning, offering a comprehensive framework for the development of scenario-specific models. This approach not only addresses the challenges identified but also sets a new benchmark for the application of machine learning in practical settings. By prioritizing customization, efficiency, and privacy, coupled with a commitment to interdisciplinary collaboration and innovation, this work significantly enhances the performance and relevance of machine learning technologies. As we venture forward, the principles delineated in this chapter are poised to inspire continued research and development, propelling the field towards unprecedented levels of excellence and impact.

*Transition Paragraph: Chapter five delves into scenario-based machine learning by thoroughly considering the information within the environment and the specific needs of the scenario, striving for balance through multi-objective optimization. Up to this point, we have discussed the more conventional and easily understandable data-level adjustments specific to scenarios. However, does scenario-based machine learning stop here? Clearly, it does not. In the subsequent chapter, we will discuss understanding and abstracting scenario from a higher dimension, penetrating the scenario with the utmost precision.*

# CHAPTER 6 MACHINE LEARNING MODELS INSPIRED BY CORE CHARACTERISTIC OF SPECIAL SCENARIOS

## 6.1 Introduction

This section will focus on the scope that traditional machine learning, which is the main target of this chapter, fails to cover, as well as some conceptual original rational analyzes of machine learning models inspired by core characteristic of special scenarios. Beginning with this chapter, we will take our thinking further and more macroscopically. It will no longer be as tightly focused on one single individual object as it was in the previous two chapters. Instead, we will focus on the common problems in the whole application scenario.

### 6.1.1 Problem Analysis

At present, research in machine learning has become one of the most sought-after directions in interdisciplinary fields, attracting scholars from diverse disciplinary backgrounds to employ machine learning techniques to drive innovation and development in their respective areas of expertise (S. Bhattacharya; M. I. Jordan & Mitchell; Littmann et al.; Ulf). Despite the vast possibilities brought forth by the wide application of machine learning technologies across various domains, there exists a prevalent and profound issue at this stage: researchers and developers often adopt an imitative strategy in the construction of machine learning models, lacking in-depth thought and innovation. They tend to follow established procedures, applying methods and models from previous research to their own datasets without delving into the underlying principles and logic (Angela, Doris, D, & Aditya; Cockburn, Henderson, & Stern; Yasuhiro et al.). This methodological shortsightedness and dependency lead to several negative consequences:

**Insufficient capture of subtle differences.** In many areas, especially those involving critical issues such as human health and environmental monitoring, traditional machine learning models often fail to effectively identify and utilize subtle differences in data (R. A et al.; Andrea, Lorenzo, A, & F; C. Ding et al.; Leonardo, Gabriel, Thomas, Maria, &

Prashant; A. M et al.; O & R; Shixuan et al.). These nuances, such as variations in patients' physiological responses or slight changes in environmental conditions, play a decisive role in the successful completion of tasks. However, due to the complexity and diversity of data, these critical pieces of information are often overlooked during the model training process, resulting in unsatisfactory performance in practical applications. Data-driven models, limited by the volume of data, struggle to ensure absolute utilization of characteristics.

**Unresolved issues of data scarcity and skewness.** In specific application scenarios, such as rare disease diagnosis or particular environmental monitoring, one of the main challenges is the severe lack of effective samples and extreme imbalance of data (Kevin et al.; Oussama et al.; "Proceedings of the 2023 6th International Conference on Machine Vision and Applications," ; K. M. Sunil et al.; Tianci et al.). Existing machine learning models perform poorly in dealing with such imbalanced data, often leading to a bias towards the majority class and neglecting predictions for the minority class. This imbalance directly impacts the models' generalizability and practical value. There is a lack of an approach that starts from core characteristic to make more effective use of limited data resources, building models that also have good discriminative power for minority samples through deep understanding and analysis of certain key characteristics (Chakravarthy, Bonthu, Chen, & Zhu; Mousavi, Shahbazi, & Asudeh; Napierala & Stefanowski; Narwane & Sawarkar; Sánchez-Marqués, García, & Sánchez).

**Lack of model interpretability.** As model structures become increasingly complex, their internal decision-making processes become harder to track and understand (Ciobanu-Caraus et al.; David & T; Lage et al.; Linardatos et al.; Molnar et al., 2020; Pablo, Mikaël, Jorge, & Bernardo; Tiwari et al.). This lack of transparency and interpretability is particularly prominent in application domains that require high levels of trust and decision explanation, such as law, healthcare, and finance . The "black box" nature of model decisions reduces users' trust in model judgments, limiting the widespread adoption and application of machine learning technology (Bhatt et al.; D. V. Carvalho, Pereira, & Cardoso; Haddouchi & Berrado; Lakkaraju & Bastani; Moss, Corsar, Shaw, Piper, & Hawthorne; Sethi, Kalia, Sharma, & Nagori, 2020; Tiwari et al.; Vipin, Shailendra, & Kumari). There is an urgent need for a way to focus models on the core characteristic of

specific scenarios, making the decision logic of models more closely aligned with the intuitive understanding of actual application scenarios, thus enhancing model transparency and interpretability.

**Insufficient ability to adapt to dynamic environments.** In practical applications, the distribution and characteristics of data may change over time, environment, and other external conditions, requiring models to have good adaptability and flexibility (Ditzler & Polikar; Fields, Hsieh, & Chenou; Firas; Manias, Chouman, & Shami; Nelson, Corbin, & Blowers; Samuel et al.; Timothée, Massimo, & I). However, traditional machine learning models are often trained and tested based on static datasets, lacking effective mechanisms to adapt to these changes, leading to a decline in long-term performance and reliability of the models (L. Adam et al.; Angeliki et al.; C. B & J; Jacob; G. L et al.; Lydia, Sarah, Esther, Max, & Moritz; Maximilian, F, Viktor, & Ana).

More seriously, this highly repetitive and innovation-lacking work mode neglects the value of existing knowledge systems across various fields, thereby wasting precious resources and potential (Changyu, Xu, Colton, Jian-yu, & Wei; Dolly & Andy; Himel & Victor; W. J, X, Shaoming, M, & Vipin; Alshehhi M & Di; Xi-Zhu & Zhi-Hua; Zhiyuan & B).

To enhance the comprehensive performance of machine learning in specific scenarios and advance the real-world deployment of machine learning models in critical decision-making processes, machine learning models inspired by core characteristic of special scenarios have emerged. This approach, by synthesizing and judging the multitude of factors within application scenarios, finds novel and ingenious entry points from a more macroscopic perspective. It formulates more precise and ingenious solutions based on the core characteristic of the scenarios. The conclusion of this chapter will analyze how machine learning models inspired by core characteristic of special scenarios address the deficiencies of traditional machine learning solutions.

### 6.1.2 Hypothesis

This chapter operates on the hypothesis that machine learning models tailored to the core characteristics of specific scenarios can achieve superior performance in efficiency, accuracy, and adaptability compared to general-purpose models. By emphasizing scenario customization and focusing on the unique features inherent to particular application domains, models can simplify complex problems, optimize resource utilization, and address persistent challenges in traditional machine learning, such as interpretability, data scarcity, and dynamic adaptability.

The foundation of this hypothesis is the assertion that leveraging domain-specific characteristics and adapting models to the requirements of specialized scenarios creates opportunities for significant advancements in:

Detection Accuracy: The ability to extract and utilize the most relevant features specific to a scenario ensures precise predictions and outcomes, especially in environments where nuanced data differences are critical. Detection Speed: By filtering irrelevant information and focusing only on anomalies or scenario-specific data, computational efficiency is greatly improved, enabling real-time performance. Adaptability: Scenario-tailored models are better equipped to handle dynamic changes in data distributions and environmental conditions, ensuring sustained performance over time. Interpretability: Simplifying models through a focus on core characteristics enhances the transparency of decision-making processes, fostering trust and user acceptance in domains where model explainability is paramount.

### 6.1.3 Defining "Domain-Specific Core Characteristics"

The term "Domain-Specific Core Characteristics" refers to the attributes or data features within a particular application domain or scenario that have a decisive impact on completing a task or achieving a specific goal. These characteristics capture the most critical information within the domain, embodying a deep understanding of the scene and a grasp of the essence of the data (Brazdil, van Rijn, Soares, & Vanschoren, 2022; Deldjoo, Bellogin, & Di Noia; Dias et al.; Dietz, Sánchez, & Bellogín; A. G & Jingjing; Westermann,

Šavelka, Walker, Ashley, & Benyekhlef, 2021; H. S. Yang, Rhoads, et al.). In essence, they are the data attributes crucial for solving problems in a specific environment, capable of significantly affecting the performance and accuracy of machine learning models.

In the context of machine learning, identifying and leveraging these core characteristics are vital for designing efficient and accurate models (G. A et al.; Aduri et al.; O. D, Dunja, & Nikola; Hadil, Lefter, & Pablo; Henry, C, V, & Oussama; Maria, Konstantina, Katia, & Adamantia; Vitor et al.). This is because they are directly linked to the model's ability to accurately capture signals most relevant to the task at hand.

### 6.1.4 Data Features and Application Approaches Related to Core Characteristics

Data related to the core characteristics of specific scenarios typically exhibit several features, which are pivotal for guiding the customization of models.

**High Relevance.** Core characteristics usually have a high correlation with the target variable (H. Li et al.; Satabdi Mishra & Pradhan; Nayak & Tantravahi; G. Qiu, Kuang, & Goel; Silva, Silva, & Nonato; J. Zhou, Arshad, Yu, & Chen). Feature engineering, including but not limited to feature selection, feature construction, and feature transformation, should be a focus in the model customization process ("AI-Driven Automated Feature Engineering to Enhance Performance of Pred ictive Models in Data Science," ; Anupama, Himanshu, & Digvijay; Bocca & Rodrigues; Ghotra, McIntosh, & Hassan; Katya; Nargesian, Samulowitz, Khurana, Khalil, & Turaga; Obaid, Hamad, Khalil, & Nassif) to ensure that the model can fully utilize the information from these core characteristics. Optimizing model performance by emphasizing these features through feature selection and weight adjustment during model training can enhance prediction accuracy due to their high relevance.

**Domain Specificity.** These data features are often unique to specific domains, containing rich domain knowledge. Integrating domain experts' knowledge and experience during model customization can facilitate the effective identification and utilization of these features (Berrar, Lopes, & Dubitzky; Björneld, Löwe, & Carlsson; G. D, M, A,

Faegheh, & Robert; Mende et al.; Ramasubramanian & Singh, 2018). This may involve employing domain-specific data preprocessing and feature engineering techniques to ensure the model fully understands and utilizes these features. Considering how to integrate cross-domain knowledge and techniques to maximize the value of core characteristics across different fields can improve the model's generalization capability and efficiency.

**High Information Density.** Core characteristics often carry a significant amount of information essential for understanding the data's essence and making accurate predictions. Architecturally, choosing models capable of handling highly relevant and information-dense features, such as deep learning models or complex ensemble learning models (Heaton; Shan et al.; Tobias & M; Y. Yang & Nenkova; Zamani & Bendersky), and optimizing them to address specific domain data features is crucial. Customizing the model may involve detailed feature engineering to mine and leverage this information, such as through feature construction and dimensionality expansion, to enhance the model's learning capability.

**Interpretability.** Compared to broader datasets, these core characteristics are usually more interpretable. Leveraging the interpretability of core characteristics to design or select more interpretable model frameworks can make the model's decision-making process more transparent and trustworthy (S. A et al.; Angati; Dr et al.; Forough, D, Jake, Jennifer, & Hanna; Timothy, Katherine, Michael, & Luca). This can involve using more transparent model structures or incorporating model explanation components, allowing end-users to understand the model's decision process and increasing model acceptance.

### 6.1.5 The relationship between domain-specific core characteristics and individual objects

The intricate and close relationship between domain-specific core characteristics and the individual objects analyzed within specific contexts is foundational to enhancing models' predictive accuracy and interpretability regarding individual entities' performance (Johansson, Sönströd, Norinder, & Boström; Lage et al.; Scott & Su-In). These core characteristics, abstracted from individuals' data, are pivotal in capturing the essential

factors influencing entities' behaviors or performances (Caroline; Peiró, Bayona, Caballer, & Di Fabio). A thorough comprehension and examination of this nexus are paramount for models' effectiveness in forecasting individual performances (Akhuseyinoglu & Brusilovsky; Granziera & Sekhposyan; Moritz, Siemsen, & Kremer; Siriram).

**Categorization of the Relationship**

**Representativeness.** The core characteristics epitomize the most significant attributes or behavioral traits of individuals in particular contexts, mirroring individual variations and commonalities and accurately depicting potential performances in specified situations (Bergman, Donovan, Drasgow, Overton, & Henning; Kandler, Zimmermann, & McAdams; Parks & Guay).

**Predictiveness.** A direct or indirect predictive correlation exists between these characteristics and individuals' future performances or states (Almlund, Duckworth, Heckman, & Kautz; C.-H. Chang, Ferris, Johnson, Rosen, & Tan; Hill, Edmonds, & Jackson; Judge & Hurst), enabling models to forecast individuals' behaviors, performances, or risks under specific conditions.

**Explanatory Power.** The interrelations among core characteristics and their connection to individual performances offer insights into behaviors within specific contexts, significantly enhancing model credibility and user acceptance.

**The Significance of Analyzing the Relationships**

**Predictive Accuracy Enhancement.** A detailed examination of this relationship facilitates the precise recognition and exploitation of performance-influencing factors, thus boosting models' predictive precision (K. Lee, Sood, & Craven; Micallef et al.; J. Zhou et al.). This examination is critical for refining feature selection and model training, ensuring the capture of vital signals.

**Model Generalization Improvement.** Grasping the relationship between core characteristics and individual entities illuminates the commonalities and disparities among different individuals or subgroups, aiding in the creation of models with superior

generalization capabilities (Esther, Theodora, B, & Michael; Katherine, Steve, & Douglas; Seedat, Crabbé, Bica, & van der Schaar; Songzi & Yuan; Rongguang Wang, Chaudhari, & Davatzikos). These models are capable of accommodating individual diversity beyond merely excelling with specific sample sets.

**Interpretability and Explainability Increase.** Elucidating this relationship can augment the decision-making process's transparency, rendering models' predictions both accurate and interpretable (Alexandra, Ignacio, Dongyu, Laure, & K; Angati; Forough et al.; "Interpretable AI Models for Transparent Decision-Making in Complex Dat a Science Scenarios," ; Zhouyuan, Zhichao, & Zhe). For sectors demanding high interpretability, like healthcare and finance, this clarity is instrumental in bolstering user trust in model predictions.

**Feature Engineering Guidance.** The relationship analysis informs the feature engineering process, enabling the identification, construction, and selection of the most impactful features on model performance (Duboue; Prado & Digiampietri; Rajput, Tripathi, & Maurya). This not only enhances model efficacy but also elevates the development process's efficiency.

### 6.1.6 The relationship between domain-specific core characteristics and scene-related information

The relationship between domain-specific core characteristics and scene-related information (beyond individual entity data) reflects a sophisticated interplay where core characteristics capture not only the inherent attributes and behaviors of entities but also deeply intertwined with external environments, situational factors, and specific scene conditions (Cummings & Stimpson; Daniels, Frank, Menart, Raymer, & Hitzler; Mangos & Hulse; Ojha et al.). A profound analysis of this nexus is vital for the creation of machine learning models tailored to the unique requirements of specific scenes, enabling an all-encompassing understanding and adjustment to the intricacies and dynamism inherent in these contexts.

**Categorization of the Relationship**

**Mutual Verifiability.** Information pertinent to the scene, such as temporal, locational, and environmental conditions, and the scene's core characteristics offer mutual verification and logical supplementation (Á et al.; M. N, Dr, & Dr; T. S, Alessandro, Francesco, & G; Y. Sunil, Raja, & Gurpreet; Ullah, R, & Shihao), collectively delineating the full spectrum of influences on individual outcomes and scene dynamics. This layered information aids in the model's ability to discern factors across a broad spectrum.

**Contextual Dependence.** Core characteristics within specialized scenes exhibit a pronounced reliance on contextual scene information. For instance, patient physiological metrics (individual characteristics) in medical diagnostic scenarios necessitate an integrated assessment alongside disease trends and local healthcare conditions (scene information).

**Dynamic Interactivity.** There exists a potential for dynamic interplay between core characteristics and scene-relevant information within specialized contexts. Environmental shifts can affect, and be affected by, the behaviors or states of individuals, suggesting a reciprocal influence.

### The Significance of Analyzing the Relationships

**Adaptability and Flexibility Enhancement.** The examination of this relationship empowers models with improved comprehension and adaptability to scene-specific shifts, facilitating more precise responses to unique scene requisites (Piratla; Sugiyama & Kawanabe; Yao). Such adaptability is especially critical in environments characterized by rapid changes in external conditions and factors.

**Predictive Precision and Comprehensiveness Boost.** Integrating individual characteristics with scene-relevant information for analytical purposes allows models to adopt a more holistic approach in understanding and forecasting scene-specific phenomena (Bosnic & Kononenko, 2011; Bosnić & Kononenko, 2008; S. Lee, Hwang, Jin, Ahn, & Park). This integrative analysis substantially elevates the precision and dependability of predictive outputs.

**Feature Engineering and Model Design Optimization.** Insight into the interconnection between core characteristics and scene information can steer more efficacious feature engineering and model design strategies (Abhijeet & Avinash; J. Peng et al.; Soviany & Soviany, 2020; Susan & Tuteja). This might necessitate models adept at processing sequential data or algorithms that account for the interplay between environmental variables and individual traits.

**Complex Scene Demands Fulfillment.** Distinct scenes present unique requirements, potentially regarding the specificity, immediacy, and interpretability of predictive results. Delving into the core characteristics and scene-related information relationship enables the development of tailored model solutions adept at addressing these intricate demands (Bertrand; Daniels & Metaxas, 2020; F. G & S; J. Peng et al.).

### 6.1.7 Leveraging core characteristics for specific scenario

Leveraging core characteristics for specific scenario requirements involves a strategic approach to customizing machine learning model algorithms within particular contexts. These strategies should fully utilize core characteristics.

**Deep Understanding of the Scenario and Identification of Core Characteristics**

Scenario Analysis. Delve into the business needs, operational environment, and their dynamic changes within the application scenario, collaborating closely with domain experts to ensure a comprehensive understanding of the context (A. Bhattacharya, Stumpf, & Verbert; Borghesi, Baldo, Lombardi, & Milano, 2020; Kerrigan, Hullman, & Bertini; Pawan Kumar & Sharma). Core Characteristics Identification. Based on the scenario analysis, identify those core characteristics crucial for the prediction task. This involves analyzing individual entities' intrinsic attributes and behavior patterns, as well as context-related external information (C. Chen, Zhao, Bian, Xing, & Liu; Galal & El-Korany; Hayashi, Prasasti, Kanamori, & Ohwada, 2016; Orji & Vassileva; Saini, Seema, & Mor).

**Optimization of Feature Engineering**

Feature Extraction and Construction. Extract identified core characteristics and construct new features as needed, potentially involving advanced data processing

techniques like time series analysis, natural language processing (Duboue; Heaton; Mumuni & Mumuni; "Time Series Data Preparation,"), or image processing to derive deep insights from raw data. Feature Selection. Employ feature selection methods (e.g., model-based selection, recursive feature elimination) to further refine the most influential features, reducing model complexity and preventing overfitting (Cawley, 2012; Ding, Yang, & Ma; Jeon & Oh; Kernbach & Staartjes, 2021).

**Customization of Model Algorithms**

Choosing the Right Model Framework. Select the most suitable machine learning or deep learning model framework based on the types and features of core characteristics (C.-W. Chang & Dinh; Richter, Khoshgoftaar, Landset, & Hasanin; Takale, Wattamwar, Saipatwar, Saindane, & Patil; Wijeyakulasuriya, Eisenhauer, Shaby, & Hanks). For instance, RNN or LSTM for time series data, CNN for image data, or ensemble learning models like random forests or XGBoost for structured data. Adjustment of Model Structure. Adjust the model's structure, such as layers, number of hidden units, or connection patterns (Adam, A, & Honglak; Arnab & Suresh; Geoffrey E. Hinton; Kaur, Kunapuli, Joshi, Kersting, & Natarajan, 2020; Yoshua & Yann), to ensure the model adequately captures the complex relationships among these features. Capturing Feature Interactions. Consider the interactions among features in the model design, possibly through feature crossing, attention mechanisms in deep neural networks (Blaž, S, N, & Matej; Siddhant et al.; W. Song et al.; Xiao et al.), etc.

**Optimization of Model Training Strategies**

Adjustment of the training process: modify the model's training process based on the features of core characteristics, such as learning rate, regularization strategies, and choice of loss function, to optimize learning efficiency. Data augmentation and expansion: for scenarios with small but significant feature datasets, consider using data augmentation or synthetic data generation techniques to expand the training set, enhancing the model's generalization capability.

**Model Evaluation and Iteration**

Customized evaluation metrics: choose or design evaluation metrics closely related to the scenario (Farkas, Szoke, & Aradi; Heidi, E, Petra, C, & Sheelagh; Lam, Bertini, Isenberg, Plaisant, & Carpendale; Paschali M, Apostolos, Remi, A, & I) to ensure the evaluation process comprehensively reflects the model's learning effect on core characteristics and its capacity to meet scenario-specific needs. Continuous iteration and optimization: based on real-world feedback and model evaluation results, iteratively refine the model (V. Chen, Bhatt, Heidari, Weller, & Talwalkar; Stumpf et al.), adjusting feature engineering and model parameters to continually enhance performance.

**Focus on Model Explainability and Transparency**

Enhancing model explainability: consider employing interpretable machine learning techniques or providing additional explanation layers for complex models (El Shawi, Sherif, Al-Mallah, & Sakr; "Interpretable AI Models for Transparent Decision-Making in Complex Dat a Science Scenarios," ; Sarvesh Koli Komal Bhat Prajwal Korade; Tiwari et al.) to help users understand how core characteristics are utilized for decision-making. By implementing these strategies, machine learning models can fully leverage core characteristics in special scenarios, improving performance, adaptability, and explainability, thereby better meeting the specific needs of those scenarios.

This cohesive strategy framework ensures machine learning models not only deeply mine and utilize core characteristics within scenarios to boost performance but also precisely align with the complex demands of specific application contexts, achieving optimized real-world deployment. Customizing models to specific scenario needs begins with a deep understanding and identification of core characteristics, requiring researchers to have a thorough insight into the scenario's inherent features and dynamics, as well as a comprehensive grasp of business processes, operational environments, and target user needs (Baltrusaitis, Ahuja, & Morency; Barua, Ahmed, & Begum; I. Pan, Mason, & Matar; Wei Zhang, Valencia, & Chang). This demands a multidisciplinary approach that combines in-depth scenario understanding, meticulous feature engineering, custom model design, and continuous iteration and optimization, aiming for precise responses to specific scenario demands. Emphasizing the refined extraction and optimization of core characteristics,

custom model design, and the close integration of models with scenario demands is the key to ensuring success.

## 6.2 The Case for Research

### 6.2.1 A Brief Description of The Application Scenario

Inspired by the core characteristic, the background is stable, the first one that came to mind was the railway system, because the tracks are relatively fixed. Moreover, trains on the railway system are aware of each other's positions, so there is no concern about mistaking another train for an obstacle. Within the railway system, we further focused on high-speed rail. The reasons are twofold: first, high-speed rail requires faster detection speeds, which highlights the advantages of our method; second, high-speed rail trains are more standardized, making it easier to install the same equipment across different trains. In simple terms, high-speed rail provides a simpler and more pure application scenario.

The burgeoning advancement of rail transit technology, particularly in the realm of high-speed rail networks, epitomizes a paradigm shift in our conceptualization and management of mass transit systems (Campos & De Rus, 2009; Vickerman, 1997). At the core of this transformation is humanity's unceasing quest to minimize spatial barriers and bolster interconnectivity. As railway systems ascend to become integral elements of both urban and interurban transportation infrastructure, they concurrently grapple with a host of emergent challenges (Givoni, 2006; X.-s. Jin, 2018). Notably, the escalation in train velocity precipitates a marked decrease in the fault tolerance levels of train control systems, thereby compressing the temporal window for effective responses to unforeseen contingencies. Among the myriad risks, track-based obstructions—ranging from stationary objects and oncoming trains to pedestrians—pose the most acute hazard to high-speed railway operations. The failure to timely identify and mitigate these obstructions could culminate in devastating outcomes (Leng, Liu, Du, Zhang, & Quan, 2019; J. Yin et al., 2017).

In their nascent stages, railways were dependent on manual oversight, signaling

mechanisms, and human-mediated interventions for obstacle detection and clearance (L. Zhou & Shen, 2011). However, the exactitude and detection range demanded by contemporary rail systems is only attainable through technological ingenuity. Coinciding with advances in technology, the transition toward automated, computer-assisted approaches for this vital task has become increasingly prevalent (Prabhakar, Kailath, Natarajan, & Kumar, 2017) (Weichselbaum, Zinner, Gebauer, & Pree, 2013; M. Yu, Yang, & Wei, 2018). Aided by the exponential growth in machine vision technologies, a cadre of robust algorithms has emerged, offering the potential for groundbreaking advancements in obstacle recognition (Budzan & Kasprzyk, 2016; D. He et al., 2021; V. D. Nguyen, Van Nguyen, Tran, Lee, & Jeon, 2016; Padilla, Netto, & Da Silva, 2020).

Yet, notwithstanding their sophisticated attributes, many of these algorithms exhibit intrinsic constraints when deployed in the specialized milieu of high-speed rail operations. Whether reliant on image-based deep learning (D. He et al., 2021; X. Wu, Sahoo, & Hoi, 2020; Z.-Q. Zhao, Zheng, Xu, & Wu, 2019), occupancy network theories (Wirges, Fischer, Stiller, & Frias, 2018), or Light Detection and Ranging (LiDAR) point-cloud clustering techniques (Roriz, Cabral, & Gomes, 2021; Y. Wu, Wang, Zhang, & Ogai, 2020), these algorithms commonly necessitate the utilization of voluminous sensor data and pre-annotated imagery. This escalating dependence on expansive training datasets, intricate computational algorithms, and high-performance Graphics Processing Units (GPUs) engenders challenges related to system scalability, operational speed, and processing efficiency. Most disconcertingly, these techniques exhibit deficiencies in terms of detection latency and the ability to identify non-standardized, 'off-whitelist' obstacles, rendering them suboptimal for high-speed rail applications.

Moreover, the migration of these methodologies to high-speed railway contexts presents formidable obstacles at the data-acquisition stage. The majority of existing algorithms are calibrated based on vehicular datasets, tailored for urban road scenarios (Dosovitskiy, Ros, Codevilla, Lopez, & Koltun, 2017; Feng et al., 2020; Gaidon, Wang, Cabon, & Vig, 2016; P. Sun et al., 2020). In stark contrast, the dataset ecosystem specific to railway systems is conspicuously underdeveloped, thereby impeding the feasibility of developing a tailored algorithmic framework capable of fulfilling the nuanced

requirements of high-speed rail applications.

Within the evolving landscape of modern railway systems, there is an acute need to close the performance gap between existing obstacle detection technologies and the escalating demands of high-speed rail operations. Specifically, this chapter acknowledges that high-speed rail environments entail unique operational conditions and specialized needs, which form the crux for problem-solving in this context. To this end, the investigation delineates an innovative trajectory. Such an innovative trajectory is precisely inspired by the core characteristics of the scenario. Once the core characteristics of this scenario are revealed, everything will fall into place.

### 6.2.2 The Core Characteristics of Obstacle Detection System for High-Speed Railways

The domain of high-speed railways encompasses a unique operational environment, wherein the continuity and fixed nature of rail paths present both challenges and opportunities for obstacle detection systems (J. Cao, Li, & Du; Z. Nan, Zhu, Zhang, Lin, & Yang). At the heart of these systems, the fundamental principle leverages the inherent stability and predictability of the railway infrastructure (Brucker, Cramariuc, Von Einem, Siegwart, & Cadena; Ristić-Durrant et al.; Simonović et al.). This underlying characteristic sets the stage for the Customized Obstacle Detection System (CODS) to achieve unparalleled precision and speed, primarily by focusing on the transient, non-repetitive elements encountered along the rail tracks—chiefly, the obstacles.

High-speed rail systems operate within a tightly controlled and largely unchanging physical landscape. The tracks and their immediate surroundings, barring minor alterations or the effects of natural wear and environmental conditions, remain consistent over time (Dan Li & Kaewunruen; Nagakura; Quaglietta, Corman, & Goverde; Setsobhonkul, Kaewunruen, & Sussman; Y. Zhu et al.). This constancy results in a significant portion of the data collected by on-board sensors during train operations being repetitive. As trains traverse the same routes repeatedly, the majority of the sensory inputs pertain to the known, static components of the railway environment. This accumulation of repetitive data, while

initially seeming advantageous, quickly becomes a redundancy. In the quest for efficiency and expediency in obstacle detection, this repetition offers an opportunity for optimization. The critical insight here is the recognition that within this sea of constant information, it is the anomalies—the unexpected or novel entities, which are of paramount interest (Bałdyga, Barański, Belter, Kalinowski, & Weichbroth; Z. Chen, Niu, Wu, Zhang, & Wang; Gasparini et al.; Kang, Sristi, Karachiwala, & Hu). These anomalies, or obstacles, represent deviations from the norm and thus pose potential risks to the safety and smooth operation of the railway system.

**Leveraging The Fixity for Enhanced Detection**

The inherent fixity of railway environments provides a double-edged sword; while it results in data redundancy, it also offers a baseline against which anomalies can be swiftly identified. It is this aspect that the CODS capitalizes on, employing a methodological approach that systematically filters out the repetitive, known quantities of the environment to spotlight and scrutinize the anomalies (Amerise & Tarsitano; Z. Cao et al., 2022; Soule, Salamatian, & Taft). This process of elimination not only streamlines the data analysis procedure but also significantly reduces the computational load on the system (Makhoul & Harb; Mukkamala, Gagnon, & Jajodia, 2000).

The operational efficiency of CODS is thus twofold. Firstly, by discarding redundant data, the system narrows its focus to exclusively analyzing potential obstacles. This targeted analysis allows for a more rapid response to emergent threats, thereby enhancing the safety protocols of the railway system. Secondly, the reduction in data processing requirements facilitates a faster throughput, ensuring that obstacle detection does not become a bottleneck in the system's overall operation.

### 6.2.3 Dataset and Evaluation Metrics

**Dataset**

Due to the limitation that the majority of available datasets only provide real-time road information without simultaneously offering standard, unobstructed road data, this chapter has collected a unique dataset with the aid of the CARLA (Dosovitskiy et al., 2017)

simulation platform to validate the custom road-based obstacle detection algorithm. This dataset serves as a benchmark for obstacle detection experiments, encompassing multiple traversals characterized by precise localization and high-definition road condition information. For both standard obstacle-free scenarios and those with obstacles, this chapter has gathered RGB camera data and LIDAR point clouds for analysis and prediction purposes. To circumvent the need for manual labeling of collected data, this chapter has also utilized CARLA's built-in semantic LIDAR sensors and semantic segmentation cameras to collect semantic information as ground truth. Due to the use of CARLA platform, the subject of recording data is vehicle rather than train.

Detailed specifications of the sensors can be found in Tables 22 and 23. The dataset contains hundreds of comparative scenarios set under various road conditions and environmental features (such as weather and lighting intensity) across multiple scene settings (Bi, Gao, Chen, Wang, & Ma; Mirza et al.; R. Song, Wetherall, Maskell, & Ralph; X. Yu & Marinov).

**Evaluation Metrics**

To assess the quality of obstacle detection, this chapter employs two conventional metrics alongside one novel metric. The conventional metrics are the Mean Intersection over Union (mIoU) and the Mean Average Precision (mAP) (D. Hall et al.; J. Tian et al.; B. Wang). The innovative metric refers to the Maximum Braking Distance (MBD), which is the distance between the vehicle and the obstacle at the moment the obstacle detection system identifies an obstruction in the vehicle's path. A greater MBD indicates the ability to detect obstacles earlier, allowing for more timely braking and other maneuvers to mitigate the risk posed by the obstruction. In addition to the quality of obstacle detection, detection speed is also a critical metric as it pertains to the timeliness of detection information and the computational demands on the hardware. This chapter measures the operational speed of the obstacle detection system in Frames Per Second (FPS). Considering the types of obstacles that may be encountered in a railway transportation system, this chapter has selected three categories of obstacle elements from the unique database: vehicles, pedestrians, and non-standard obstacles (Chernov A, M, A, & Petr; Danijela, Marten, & K; Fabian, P, Harish, Akke, & Christian; R. M, N, & F; S. M et al.). These categories have been evaluated on the collected benchmark dataset.

Table 22. RGB Camera Parameter Settings

| Blueprint attribute | Type | Setting | Description |
|---|---|---|---|
| bloom_intensity | float | 0.675 | Intensity for the bloom post-process effect, 0.0 for disabling it. |
| fov | float | 105 | Horizontal field of view in degrees. |
| fstop | float | 1.4 | Opening of the camera lens. Aperture is 1/fstop with typical lens going down to f/1.2 (larger opening). Larger numbers will reduce the Depth of Field effect. |
| image_size_x | int | 960 | Image width in pixels. |
| image_size_y | int | 540 | Image height in pixels. |
| iso | float | 100 | The camera sensor sensitivity. |
| gamma | float | 2.2 | Target gamma value of the camera. |
| lens_flare_intensity | float | 0.1 | Intensity for the lens flare post-process effect, 0.0 for disabling it. |
| sensor_tick | float | 0 | Simulation seconds between sensor captures (ticks). |
| shutter_speed | float | 200 | The camera shutter speed in seconds (1.0/s). |

Table 23. LiDAR Parameter Settings

| Blueprint attribute | Type | Setting | Description |
|---|---|---|---|
| channels | int | 32 | Number of lasers. |
| range | float | 30 | Maximum distance to measure/raycast in meters. |
| points_per_second | int | 90000 | Points generated by all lasers per second. |
| rotation_frequency | float | 40 | LIDAR rotation frequency. |
| upper_fov | float | 10 | Angle in degrees of the highest laser. |
| lower_fov | float | -30 | Angle in degrees of the lowest laser. |
| horizontal_fov | float | 360 | Horizontal field of view in degrees, 0 - 360. |
| atmosphere_attenuation_rate | float | 0.004 | Coefficient that measures the LIDAR instensity loss per meter. Check the intensity computation above. |
| dropoff_general_rate | float | 0.45 | General proportion of points that are randomy dropped. |
| dropoff_intensity_limit | float | 0.8 | For the intensity based drop-off, the threshold intensity value above which no points are dropped. |
| dropoff_zero_intensity | float | 0.4 | For the intensity based drop-off, the probability of each point with zero intensity being dropped. |
| sensor_tick | float | 0 | Simulation seconds between sensor captures (ticks). |
| noise_stddev | float | 0 | Standard deviation of the noise model to disturb each point along the vector of its raycast. |

### 6.2.4 Related Work

This section critically surveys recent technological advancements in obstacle detection systems, particularly within the domain of autonomous vehicles. It delves into the evolution of visual signal processing, the integration of LiDAR in detection, and the advancements in sensor fusion methodologies. Each segment not only underscores pivotal developments but also interrogates their limitations, establishing the context for the proposed research.

**Visual Signal Advancements in Autonomous Vehicle Detection**

(1) Emergence of Real-time Detection Frameworks

The emergence of real-time detection frameworks signifies a quantum leap in autonomous vehicle technologies. Convolutional Neural Networks (CNNs) have been paramount in feature hierarchy extraction (S. Peng, Niemeyer, Mescheder, Pollefeys, & Geiger, 2020; Sultana, Sufian, & Dutta, 2020), with architectures like Faster R-CNN (Girshick, 2015; Ren, He, Girshick, & Sun, 2015), SSD (W. Liu et al., 2016), and YOLO (P. Jiang, Ergu, Liu, Cai, & Ma, 2022; Redmon, Divvala, Girshick, & Farhadi, 2016; Terven & Cordova-Esparza, 2023) propelling the field forward. However, the pursuit of precision set by the Faster R-CNN series of architectures impacts their practicality in high-speed scenarios. Although the highly time-consuming selective search algorithm was eventually replaced by the Region Proposal Network (RPN) in Faster R-CNN, the approach of identifying objects post-detection still limits its application in dynamic environments. The one-stage algorithms, SSD and YOLO, attempt to address this by integrating localization and identification in a single step using global information. Yet, this undiscriminating computation of global data heightens hardware requirements; it is resource-intensive and not conducive to deployment on edge devices. Despite the rapid progress in computational power, there remains a need for improvement in detecting smaller objects. If global information could be rapidly filtered, one-stage algorithms could unleash greater potential.

(2) Integration of Transformers and Attention Mechanisms

DETR (Detection Transformer) represents a paradigm shift by leveraging transformers to circumvent the need for heuristically-based Region Proposal Networks,

thereby streamlining the detection process. Furthermore, the introduction of attention mechanisms breaks free from the constraints of CNNs, focusing more effectively on the interrelations within images. This approach tightly integrates object detection with background information, enhancing the overall contextual understanding (Carion et al., 2020). In addition to DETR, approaches like the Vision Transformer (ViT (K. Han et al., 2022)) and Swin Transformer (Ze Liu et al., 2021) further refined the application of self-attention mechanisms, addressing challenges related to the size of the model's receptive field and the encoding of positional information in images. By learning global dependencies across the entire image, these models have demonstrated impressive performance in object detection tasks (S. Khan et al., 2022). Moreover, the incorporation of attention mechanisms has been pivotal in enhancing model interpretability and focus (Chefer, Gur, & Wolf, 2021; B. Pan et al., 2021). Limitations. Despite their success, transformers and attention-augmented models require significant data and computational time for training, which can be a bottleneck for applications necessitating rapid deployment and adaptation. Because they are often designed with a focus on maximum accuracy rather than real-time processing efficiency (Y. Li, Mao, Girshick, & He, 2022).

**LiDAR-Based Detection Advances**

(1) Clustering Techniques in Detection

In the realm of LiDAR-based target detection, traditional methodologies have predominantly utilized clustering algorithms. Among these, DBSCAN (Density-Based Spatial Clustering of Applications with Noise) has been a cornerstone, celebrated for its proficiency in delineating clusters of arbitrary shapes by leveraging density metrics (K. Khan, Rehman, Aziz, Fong, & Sarasvady, 2014; Schubert, Sander, Ester, Kriegel, & Xu, 2017). Concurrently, Euclidean Clustering has emerged as an effective means to assemble point clouds into discernible structures, primarily governed by spatial proximity. Furthermore, the HDBSCAN (Hierarchical DBSCAN) extends DBSCAN's capabilities, allowing variable density cluster identification, crucial in complex environments (McInnes, Healy, & Astels, 2017). But, these clustering algorithms, while effective for pattern recognition, often struggle with varying densities and noise in data, leading to a potential compromise in detection accuracy. This is where the RANSAC (Random Sample Consensus) algorithm emerges as a noteworthy alternative (Chum, Matas, & Kittler, 2003;

Derpanis, 2010; Schnabel, Wahl, & Klein, 2007). RANSAC excels in its robustness against outliers in noisy data, leveraging a probabilistic approach to model fitting that iteratively identifies and excludes anomalies. This characteristic renders it highly effective in environments where data integrity is compromised. However, its performance is contingent on the correct estimation of inlier thresholds and the proportion of outliers, which can be challenging to ascertain precisely. Additionally, RANSAC's iterative nature can lead to computational inefficiencies, especially in cases with high-dimensional data or large datasets. The inherent trade-off between speed and accuracy renders traditional numerical computation-based methods inadequate for meeting the demands of real-time dynamic object detection.

(2) Deep Learning in LiDAR Detection

PointNet, as initially introduced by Charles R Qi et al. (Charles R Qi, Su, Mo, & Guibas, 2017), and further explored in subsequent studies, has established a foundational role in employing deep learning for feature extraction from point cloud data (Y. Li et al., 2020; Zamanakos, Tsochatzidis, Amanatiadis, & Pratikakis, 2021). Its successor, PointNet++ (Charles Ruizhongtai Qi, Yi, Su, & Guibas, 2017), has advanced this domain by addressing the inherent limitations identified in PointNet. This evolution is particularly notable in its enhanced capability for feature learning, achieved through the implementation of hierarchical neural networks. These networks are intricately designed to capture the local structures inherent in the metric space of the input points, thereby facilitating a more nuanced data analysis. Despite these technological strides, both PointNet and PointNet++ are not without their challenges. These models typically necessitate substantial computational resources for effective training and inference processes. Furthermore, their performance is susceptible to deterioration under adverse weather conditions. Such conditions can adversely affect LiDAR returns, leading to issues of data sparsity and compromised model accuracy (Mahmudul Hasan et al., 2022). There is an urgent need for a point cloud-based object detection method that offers high robustness and real-time capabilities to meet related demands.

**Advances in Sensor Fusion for Detection**

(1) Emergence of Occupancy Networks

Occupancy networks have provided nuanced environmental representations, enabling

detailed detection through probabilistic modeling of space occupancy (L. Han, Zheng, Xu, & Fang, 2020; Mescheder, Oechsle, Niemeyer, Nowozin, & Geiger, 2019). These methods, like OctoMap (Hornung, Wurm, Bennewitz, Stachniss, & Burgard, 2013; Li Sun, Yan, Zaganidis, Zhao, & Duckett, 2018; Liang Zhang et al., 2018) and VoxNet (Maturana & Scherer, 2015; Shen & Stamos, 2020), have shown promise in generating 3D occupancy grids with high resolution from various sensor inputs. Despite their detailed spatial representations, these networks are often challenged by the dynamic nature of environments in real-time scenarios.

(2) Evolution of Sensor Fusion Methodologies

Sensor fusion (Zhong et al., 2021) has progressed with approaches like DeepFusion (Y. Chen, Li, Ghamisi, Jia, & Gu, 2017; Yingwei Li et al., 2022; Shivakumar et al., 2019; Tu et al., 2021), which intelligently combines features from different sensor modalities, and FusionRCNN (X. Xu et al., 2023), which merges region-based CNNs with multiple sensor data for enhanced detection accuracy. Additionally, methods such as AVOD (Aggregate View Object Detection (Ku, Mozifian, Lee, Harakeh, & Waslander, 2018)) provided a mechanism to fuse 2D image and 3D LiDAR data for object detection tasks. While these advanced sensor fusion techniques have improved detection capabilities, they still face significant challenges when confronted with sensor noise, occlusions, and the high variability of objects in size and shape. These factors can degrade the performance of fusion-based systems, leading to potential safety risks in autonomous navigation. In conclusion, the lack of sufficient data in the railway system makes it difficult to support the training needs of fused sensors.

**Persistent Challenges in Detection**

Notwithstanding these advances, the quest for real-time, accurate, and robust detection in diverse conditions persists. Addressing small object detection, enhancing computational efficiency, and fortifying detection robustness against environmental fluctuations remain as formidable challenges. In response to the practical demands of the railway system, there is an urgent need to develop an obstacle detection algorithm characterized by high real-time performance and sensitivity, and one that does not rely on extensive manually annotated training data. These unresolved issues underscore the imperative for novel solutions, such as the Customized Obstacle Detection System (CODS),

conceived to overcome these hurdles within high-speed railway contexts.

## 6.3 A Framework of Customized Obstacle Detection System (CODS)

The study stands as particularly impactful because it circumvents traditional pitfalls by leveraging the distinct features of high-speed railways. This chapter introduces a "Customized Obstacle Detection System", thereby eschewing reliance on cumbersome datasets and computations. Since the core characteristics of this application scenario have been analyzed in section 6.2.2. And a conceptual upgrade of the obstacle detection system inspired by the core characteristics has been made. The next major work is how to realize this concept. The cornerstone of the approach is the exploitation of real-time sensor data and predetermined background information to pinpoint anomalies. A comprehensive comparison between traditional object detection approaches and the **Customized Obstacle Detection System (CODS)** is depicted in Figure 30.

The methodology comprises two pivotal phases: the iterative refinement of a "Standard obstacle-free maps" and the real-time identification of obstacles through comparative analysis of deviations. Generated automatically through the aggregation of sensor data from in-service trains, the standard obstacle-free maps are dynamically updated in a self-supervised manner. This standardization allows for the seamless incorporation of timely and relevant track data. During live operations, segments of this map, corresponding to fixed-length sections of actual tracks, serve as reference points. As a train traverses the railway, the system juxtaposes real-time sensor readings with these reference segments to identify any discrepancies, thereby flagging potential obstacles.

By employing this iterative methodology, the system not only accelerates the rate of obstacle detection but also elevates its sensitivity. Moreover, it ensures that the standardized obstacle-free road map remains both comprehensive and current, thereby significantly contributing to the advancement of safety and efficiency in high-speed railway systems.

This chapter substantiates that the track-specific customization approach can be

seamlessly integrated into existing high-speed railway infrastructures, resulting in marked enhancements in both the speed and detection coverage of obstacle identification. Experimental validation carried out on a dataset gathered from the Carla simulation environment manifests a noteworthy performance upswing, achieving 10% increase in detection mean average precision and a maximum improvement of 75% in detection speed.

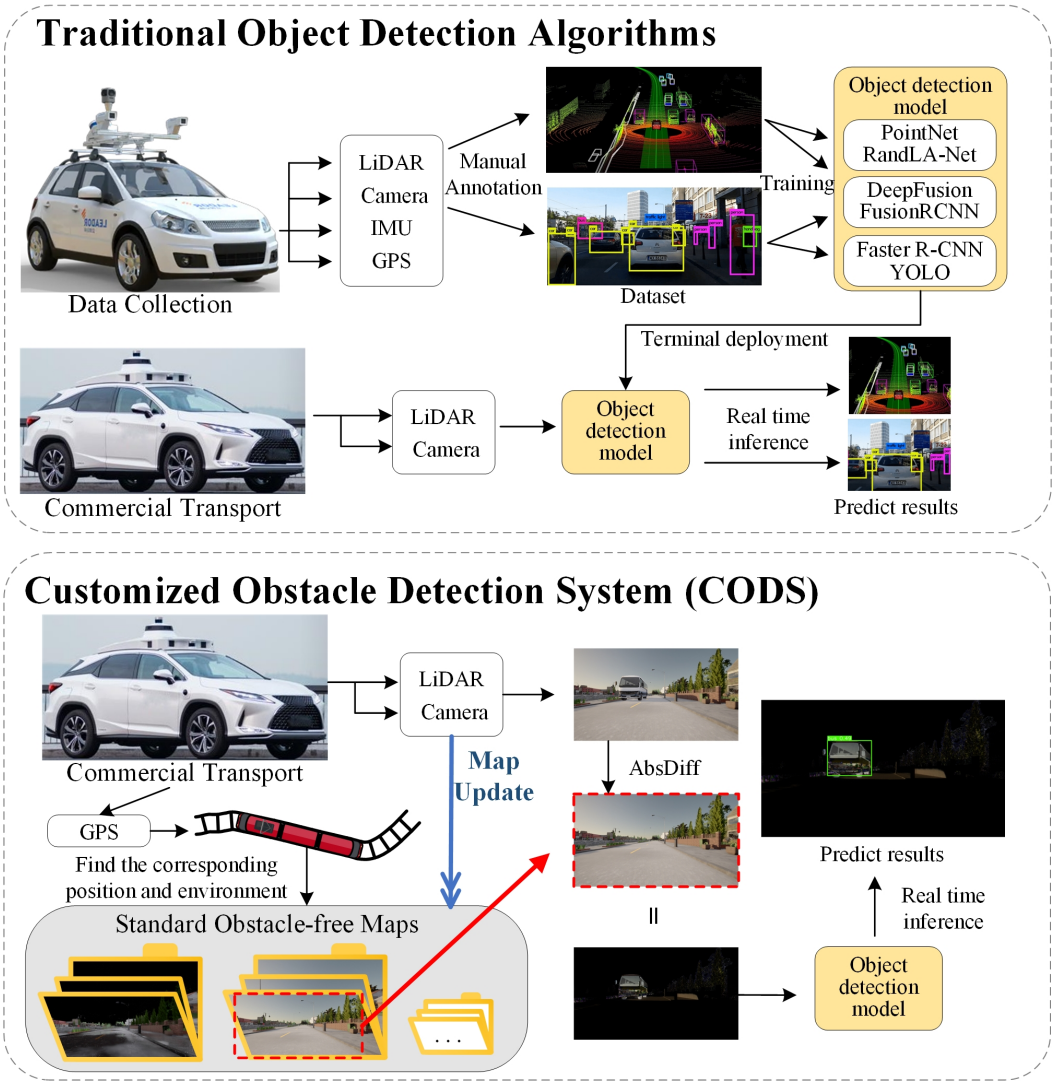



*Figure 30. Comparison of full process methods for obstacle detection systems.*

Note: Traditional detection systems contain complex manual labelling sessions and do not support timely updates. It completely relies on the comprehensiveness of the collected data and is prone to the influence of irregular objects, and objects outside

the whitelist. This chapter proposes the Customized Obstacle Detection System, an innovative solution method that aims to help identify obstacles through customized information. It will be continuously updated as the standard obstacle-free map is continuously integrated with new observations from operating trains.

## 6.4 Specific Solutions

The aim of this study is to bolster the efficacy of real-time obstacle detection by leveraging standard obstacle-free maps. Toward this end, this chapter introduces a system framework, as illustrated in Figure 31. The figure presents the system that utilizes the RGB camera for input. The methodology for the system that processes LiDAR signals is parallel in nature and is omitted here to maintain conciseness. This framework is meticulously crafted to simultaneously facilitate the training of global standard obstacle-free map updates and the functioning of the local obstacle detection system, seamlessly integrating a fusion component.

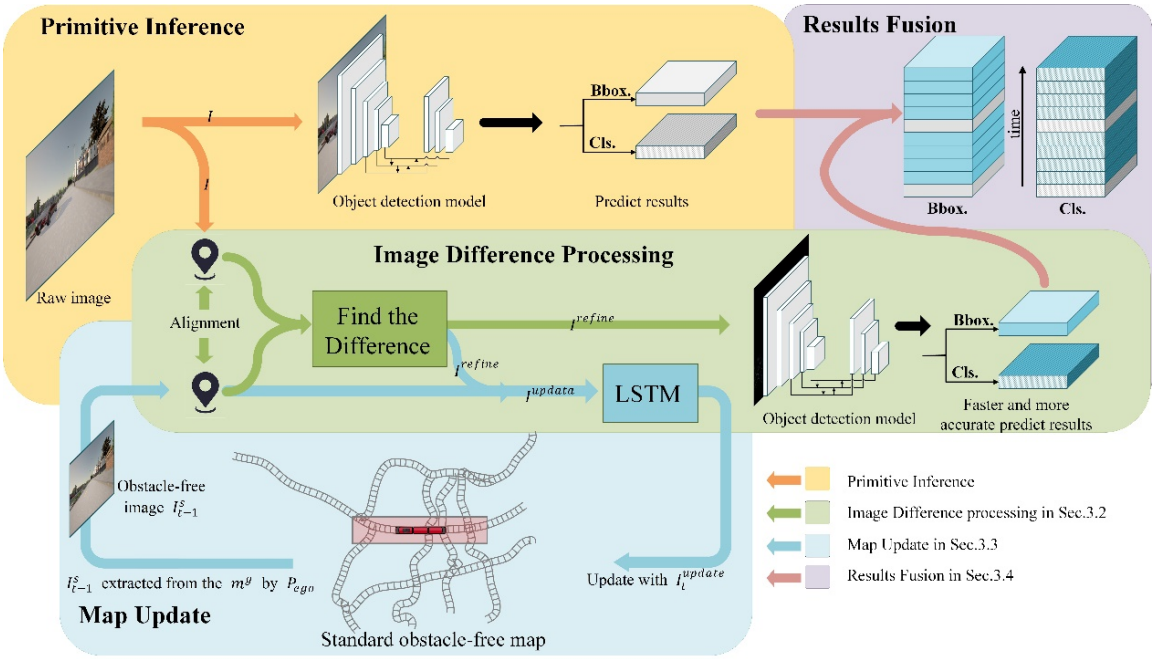



*Figure 31. The architecture of the Customized Obstacle Detection System (CODS).*

Note: The top yellow box includes the traditional obstacle detection process. The

green box contains the core information differential processing module, which is designed to improve the efficiency of information processing. The refined information continues to flow both to the subsequent object detection model and to the blue map update module. In the blue box at the bottom, the CODS queries the obstacle-free information corresponding to the current one from the obstacle-free standard maps. The purple result fusion module accepts result information from both sources for fusion to improve information density.

This chapter is primarily divided into four sections. The first section presents the problem setup, clearly defining the issues under discussion from a mathematical perspective and establishing definitions for various concepts and symbols referenced later in the text. The second and third sections represent the core innovations of this study, detailing the methodologies for calculating the difference between pieces of information and the approaches for constructing and maintaining the standard obstacle-free map, respectively. The fourth section supplements the overall discussion with additional details pertinent to the operation of the entire system.

### 6.4.1 Problem Setup

The system is tailored for conventional target identification tasks and is outfitted with an array of onboard sensors including cameras, LiDAR, and GPS/IMU (Inertial Measurement Unit) for precise positioning. Consistent with the configuration depicted in Figure 31, the subsequent section will focus exclusively on the system that employs the RGB camera, although the LiDAR detection system is analogous. This chapter adopts a single-frame setting, intentionally eschewing the incorporation of time-related contextual data. This research utilizes a standard object detection model, herein referred to as $F_{\text{Detect}}$, to process and predict image data. Furthermore, this chapter has established and continues to manage a comprehensive global map, the specific parameters of which are detailed subsequently.

Under the single-frame setting, each observation consists of input from the cameras $I \in R^{h \times w}$ (where $h$ and $w$ denote the size of the figure). And the ego train's position in

the global coordinate system $P_{ego} \in R^{L \times C \times E}$, where $L$ and $C$ represent the total number of railway lines and the completion that follows a particular track forward, respectively. $E$ is more specific and is a scalar that describes the current environmental factors at that location. Additionally, this research creates and maintains a standard global map $m^g \in R^{h \times w \times L \times C \times E}$. That is, there is an observation at each location in the map.

Initially, this research acquires the local features, including bounding boxes, label index and confidence:

$$BBox, LIn, Con = F_{Detect}(I) \tag{56}$$

This chapter finds the standard image information, $I^s$ corresponding to the current position from the map $m^g$, through the position $P_{ego}$ from $m^g$. A difference function is then applied to the standard road information $I^s$ and the locally acquired real-time road information $I$ to generate a refined road image. Road information can be images or point cloud data.

$$I^{refine} = F_{diff}(I, I^s), I^{refine} \in R^{h \times w} \tag{57}$$

Finally, object detection model, such as YOLO, computes the detection output from the refined ROAD IMAGE at a faster running speed.

$$BBox_{refine}, LIn_{refine}, Con_{refine} = F_{Detect}(I^{refine}) \tag{58}$$

Simultaneously, the global map is updated. The global map utilizes external memory and computational power to incrementally integrate new information while providing knowledge output. This dual function ultimately enhances local map estimation performance. These outputs, $BBox_{refine}, LIn_{refine}, Con_{refine}$, are layered in sequence with the unprocessed road information detection outputs $(BBox, LIn, Con)$ in a predetermined ratio, producing more informative data for the intelligent driving system. This part of the information fusion can be referred to in the results fusion section in Figure 31. The entire process is described in Algorithm 3 in appendix.

### 6.4.2 Difference Processing Methods

In the assumptions of this study, it is necessary to simplify the real-time detected road information data, retaining only information about obstacles and eliminating background

information that does not pose a risk during driving. The critical issue then becomes how to utilize the standard information without obstacles stored in the map. This subsection will begin with an analysis of the simplest scenarios, subsequently increasing the complexity of the scenarios to demonstrate the principles and feasibility of the algorithm.

**Visual Signals (RGB Camera)**

In the realm of computer vision, the advantages of RGB cameras are undeniably prevalent (Wiley & Lucas, 2018). The stability and affordability of RGB cameras have established them as one of the most essential tools in the field of vision. The foremost advantage of RGB cameras in this study is their accessibility in detecting spatial information over greater distances. Collecting information from afar lays the groundwork for high-speed trains to execute emergency braking at extremely high velocities (Chapel & Bouwmans, 2020).

This chapter posits a near-ideal scenario on a segment of laboratory track where all environmental factors remain constant. With fixed lighting and set design, the data recorded by the onboard cameras as the train repeatedly traverses the laboratory track should be identical. This research stores a complete recording of a trip in a global map, utilizing this as a reference for standard obstacle-free road information. When the train is driven on the track again, the real-time data acquired should, theoretically, be in complete concordance with the standard obstacle-free road information from the global map—that is to say, the difference should be zero.

Next, this chapter modified the laboratory track by placing fixed utility poles alongside the rails and positioning a dummy signboard on the distant tracks. The train was then set to travel the track again, and the data recorded in real time was compared once more with the standard road information. At this point, the two sets of information diverged, as the real-time data now included additional imagery of the utility poles and the dummy signboard. If the aim was to streamline the real-time data, the ideal outcome would involve isolating only the information pertaining to the dummy and the poles. The pivotal question arises: how can we effectively condense the real-time information using the standard road information as a reference? To minimize computational time, complex algorithms should

be eschewed. After a series of exploratory trials, image differencing is selected as a comparatively ideal method. As the name suggests, image differencing involves subtracting the corresponding pixel values of two images, thus attenuating the similar parts of the images and accentuating the altered sections. The calculation is formalized in Equation (59):

$$\text{output}(\text{I}) = \text{saturate}(\,|\text{input}_1(\text{I}) - \text{input}_2(\text{I})|\,) \tag{59}$$

Since RGB images consist of three channels, each channel is processed independently during calculation. Taking the absolute value of the differencing result ensures the significance of both the real-time transmitted data and the standard road information is maintained, reducing the possibility of information loss. The results are further processed with a saturate function to ensure the computational output represents meaningful numbers that do not exceed the predefined range (Bradski, 2000).

After such an image differencing operation, the resultant image predominantly displays black areas (regions devoid of any information), with the obstacles added appearing in isolated regions, as illustrated in the fourth row of Figure 33. When these processed images are fed into subsequent computer vision object detection models, they can significantly reduce the computational time required for object detection. Furthermore, this computation involves only matrix subtraction, and the processing time within the information workflow does not exceed three milliseconds, thus having a negligible impact on the overall computation speed. A detailed quantitative analysis is contented in the experimental section.

The discussion of visual signals in simple scenarios presented thus far is overly idealized and significantly diverges from real-world settings. This is due to the complexity of scene-related factors encountered in reality, most commonly including variations in lighting, weather, and seasons. These variables can lead to minor changes reflected in the positioning of shadows, overall scene brightness and visibility, cloud formations in the sky, and even the slight swaying of plants with the wind. All these factors contribute to the inclusion of extraneous information in the results of image differencing computations that are unrelated to actual obstacles. Such information can be mitigated through various image

processing techniques, such as setting thresholds to filter out areas with minimal brightness variation or by eliminating regions of minor changes. However, due to the need for numerous hyperparameter adjustments—such as thresholds for brightness changes—these methods fail to accommodate all scenarios comprehensively. The most effective strategy is to focus exclusively on areas accessible to the train, namely, the railway tracks and the space above them. Given that railway tracks follow a fixed route, whether it involves real-time visual signal analysis to define the scope of the railway tracks or marking the extent of the tracks in each image as a constant within the global map, both are feasible tasks.

Additionally, certain stable scene transitions, such as those resulting from seasonal changes, can be managed by creating global maps of standard road information for the same location under different environments. In practice, the appropriate image from the global map is selected based on real-time conditions to conduct image differencing. The specific methodologies are detailed in section 6.5.3.

**Point Cloud Signals (LiDAR)**

The acquisition of point cloud datasets is predominantly conducted via LiDAR scanners, capturing an unordered and unstructured aggregation of voluminous data points within a three-dimensional matrix (Raj, Hanim Hashim, Baseri Huddin, Ibrahim, & Hussain, 2020; Wandinger, 2005). Each datum inherently encodes the spatial distribution of the objects in question. The intrinsic fidelity of point cloud data enables a more precise depiction of object placement within a spatial context than is feasible with two-dimensional imaging, coupled with an inherent stochasticity in its acquisition. The disorderly and unstructured nature of point cloud data, along with its considerable size, introduces formidable challenges to real-time data processing endeavors (V.-H. Cao et al., 2015; Lv et al., 2017; Pfeifer & Böhm, 2008). Nonetheless, inspired by prior examinations into differencing-based obstacle localization, the application of differencing techniques to point cloud information emerges as a logical progression.

Similar to the procedures outlined in 6.5.1 visual signals (RGB camera) part, the treatment of point cloud information is notably straightforward. The process involves a simple subtraction of the standard obstacle-free road point cloud data from the real-time

point cloud data. The residual point cloud spatially delineates the loci of the obstacle. This differencing computation can be efficiently carried out by GPUs with ample memory, showcasing a formidable speed superiority when compared with conventional segmentation approaches that rely on mathematical modeling and geometric inference, or segmentation via feature descriptors.

Considering the stochastic nature of point cloud distributions, the standard obstacle-free road information, which is subject to subtraction, should be conservatively augmented in real-world operations. That is to say, the immediate spatial vicinity of each data point within the real-time information point cloud representing standard road information ought to be excised. The magnitude of this neighboring space, a variable adjusted according to the specifications and performance of the lidar apparatus, acts as a real-application parameter. This method of accommodating for indeterminate information is particularly adept at screening out minuscule spatial fluctuations attributable to environmental dynamics, such as the differential point cloud locations engendered by the movement of foliage. The difference operation of the point cloud is shown as formulated in Equation (57), this functionality was implemented by Open3D (Q.-Y. Zhou, Park, & Koltun, 2018).

$$\text{distances} = \text{PointClond}_{\text{real-time}}.\text{compute\_point\_cloud\_distance}(\text{PointClond}_{\text{standard}})$$

$$\text{distances\_array} = \text{numpy}.\text{asarray}(\text{distances})$$

$$\text{Index}_{\text{obstacle}} = \text{numpy}.\text{where}(\text{distances\_array} > \text{Th})[0]$$

$$\text{PointClond}_{\text{obstacle}} = \text{PointClond}_{\text{real\_time}}.\text{select\_by\_index}(\text{Index}_{\text{obstacle}})$$

### 6.4.3 Standard Obstacle-free Map

In the preceding section, this chapter has ascertained what types of information need to be stored in the maps. Moving forward, it is time to discuss the methods of accessing and updating this information.

**Accessing the Standard Obstacle-free Map**

Compared to traditional high-precision maps, standard obstacle-free maps contain a plethora of details; one might even argue that they are a re-creation of the world. This

results in an immense volume of data within the standard obstacle-free maps. Transferring all this information to the train before departure would pose a significant challenge to the train's onboard data storage capabilities.

Furthermore, the real-time data collected by each train while traveling on fixed tracks can be tremendously beneficial to other trains operating on the same route. This is especially true when the data collected by earlier trains about potential obstacles can be shared promptly with trains departing later. Such timely information exchange can be instrumental in planning overall road operations and ensuring the safety of subsequent trains. Considering these needs, it would be ineffective to wait until a train completes its route to synchronize the data with the standard obstacle-free map, due to the poor timeliness of such a process.

Considering the above requirements for data transfer in both upload and download directions, this study proposes a distributed storage method for standard obstacle-free maps. This method involves dividing each long route into fixed-length short segments and placing high-speed storage stations at the junctions of these segments. When a train approaches a new short segment, the train's obstacle detection system automatically downloads the standard obstacle-free map for the upcoming segment from the high-speed storage station. Concurrently, it transmits the real-time road information collected from the preceding segment to the storage station.

After completing this series of automatic uploads and downloads, the obstacle detection system can utilize the newly downloaded standard obstacle-free map to detect obstacles on the next road segment. In tandem, the high-speed storage station updates the standard obstacle-free map for the previous segment with the real-time information gathered, thus preparing it for use by upcoming trains.

Since the real-time data involved in map updating is only a very small percentage of the collected data, data transfer remains easy even at HD (High Definition) resolutions and high frame rates. Which image information needs to be involved in more detail will be analyzed in the next section.

**Updating the Standard Obstacle-free Map**

Before delving into the methodologies for updating the standard obstacle-free map, it is essential to discuss the principles and significance of these updates. The accuracy of such a map is critical, as it pertains to the safety of life and property. To ensure this accuracy, map updating must be approached with caution. Changes to the road of significant magnitude should not be carelessly transmitted to the standard obstacle-free map by any train. Furthermore, the purpose of updating the road map is not to incorporate observed obstacles as part of the environmental backdrop, but rather to gradually integrate long-term environmental changes. With this objective clarified, it becomes apparent that the portions of the map requiring updates are those without significant changes. By establishing a fixed threshold for changes, images with variations below this threshold contribute to the map's update with a fixed weight. In practice, the detection system applies a blank mask over the sections of the image with changes exceeding the threshold—that is, parts that the system identifies as obstacles—where all channel values in this mask are set to zero.

For images exhibiting substantial changes, there are generally two scenarios to consider. One scenario involves obstacles that are reported consistently by multiple trains, which should be addressed by the railway's mobile forces to remove any impediments to travel. These images containing obstacles need not be included in the update of the standard map. The second scenario involves significant changes due to updates in fixed installations like buildings and signs surrounding the road. Such updates should be confirmed by railway infrastructure protection personnel before integrating this new information into the map.

In the specific implementation of map updates, two time-related models, GRU (Gated Recurrent Unit (Chung, Gulcehre, Cho, & Bengio, 2014; Dey & Salem, 2017)) and LSTM (Long Short-Term Memory) (Hochreiter & Schmidhuber, 1997; Van Houdt, Mosquera, & Nápoles, 2020), were preliminarily considered. The GRU represents a simpler updating strategy; however, for enhanced controllability, this study has selected LSTM as the operational model for map updating. By setting parameters for specific temporal intervals within the LSTM, manual control over the extent of map updates can be achieved. This is advantageous when rapid and significant map alterations are necessary to accommodate swiftly changing background environments. Additionally, LSTM is capable of actively

deleting certain records, allowing for the removal of sensitive or erroneous information.

The details are as follows: A single-frame local standard obstacle-free image $I_{t-1}^{s}$, which updated at $t-1$, are extracted from the global map $m_{t-1}^{g}$. The refined road information generated by the differencing operation are denoted as $I_t^{refine}$. So, subtract $I_t^{refine}$ from the real-time image data $I_t$ to get the background information $I_t^{update}$ needed to participate in the update. Integrating $I_t^{update}$ with the local standard obstacle-free image $I_{t-1}^{s}$, the LSTM yields the new local standard obstacle-free image $I_t^{s}$ at time t. Subsequently, $I_t^{refine}$ are passed through the following object detection model to predict the obstacles. And $I_{t-1}^{s}$, which is already in the global standard obstacle-free map $m^{g}$, is directly replaced by the newly generated image $I_t^{s}$. Let $\Gamma_u$ denotes the update gate, $\Gamma_f$ the forget gate, $\Gamma_o$ the output gate, $\sigma$ the sigmoid activation function, $W_*$ and $b_*$ the corresponding neural network parameters, and $\odot$ the Hadamard product. With the following operations, the LSTM fuses $I_t^{update}$ with the Local standard obstacle-free image $I_{t-1}^{s}$.

$$\Gamma_u = \sigma\left(W_u \cdot \left[I_{t-1}^{s}, I_t^{update}\right] + b_u\right) \tag{60}$$

$$\Gamma_f = \sigma\left(W_f \cdot \left[I_{t-1}^{s}, I_t^{update}\right] + b_f\right) \tag{61}$$

$$\Gamma_o = \sigma\left(W_o \cdot \left[I_{t-1}^{s}, I_t^{update}\right] + b_o\right) \tag{62}$$

$$\widetilde{C_t^{l}} = \tanh\left(W_m \cdot \left[I_{t-1}^{s}, I_t^{update}\right] + b_m\right) \tag{63}$$

$$C_t^{l} = \Gamma_u \odot \widetilde{C_t^{l}} + \Gamma_f \odot C_{t-1}^{l} \tag{64}$$

$$I_t^{s} = \Gamma_o \odot \tanh\left(C_t^{l}\right) \tag{65}$$

Within the LSTM, the update gate $\Gamma_u$, forget gate $\Gamma_f$ and output gate $\Gamma_o$ are instrumental in determining the fusion of information from the previous traversal (i.e., local standard obstacle-free image $I_{t-1}^{s}$) with the current refined data$I_{refine}$. Furthermore, they govern the incorporation of information from the current refined real-time data $I_t^{refine}$ into the global standard obstacle-free map. LSTM enables the model to better adapt to various road conditions and mapping scenarios more effectively.

### 6.4.4 Supplementary Settings for Obstacle Detection Systems

To enhance the implementation of the obstacle identification system proposed in this chapter, this section will analyze and explain some of the implementation details and techniques.

**Alignment of Standard Obstacle-Free Data with Real-Time Data**

For the system to accurately reflect obstacles by computing the differences between standard and real-time data, aligning real-time data with the corresponding standard road information at the same location is crucial. In theory, if all trains were identical in size and all cameras were installed at precisely the same position, then the real-time data collected at any point along the route would correspond exactly with the images at the corresponding positions on the standard road map, eliminating the need for alignment. However, due to variations in train models and production batches, as well as differences in the angles and positions of camera installations, the real-time data collected cannot be directly matched with the corresponding images in the standard obstacle-free map. Without effective alignment, it is meaningless and almost entirely ineffective to process image differentials between real-time data and a slightly deviated standard dataset. Therefore, to achieve alignment, calibration near high-speed data storage stations must be conducted with the aid of inertial sensors, satellite signals, and wheel speedometers. The flowchart for this subsection is shown in Figure 32.

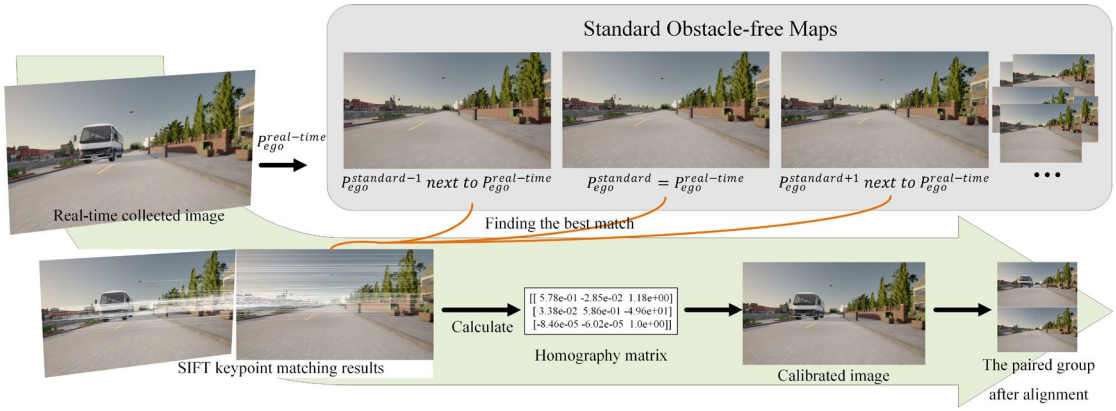



*Figure 32. Flowchart of alignment of standard obstacle-free data with real-time data.*

The specific implementation of calibration involves using the real-time collected

image $I$ as a basis to find the most similar picture in the standard obstacle-free map and aligning it through rotation and translation. First, based on the real-time image and its corresponding spatial positions $P_{ego}$, images from the standard obstacle-free map at the corresponding spatial and adjacent positions are selected. Then, the Scale Invariant Feature Transform (SIFT) algorithm (Lindeberg, 2012; Lowe, 2004) is utilized to extract key points and their corresponding feature descriptors from both the real-time images and the standard road images.

After obtaining the key points and feature descriptors, the real-time images are paired with candidate standard road images to form groups of potential matches. The similarity of the key points within these candidate groups is calculated using the K-Nearest Neighbors (KNN) algorithm (Laaksonen & Oja, 1996; Peterson, 2009). When the degree of similarity exceeds a predefined threshold, the pair with the highest similarity is chosen as the match; if the similarity within all candidate groups falls below the threshold, more images from nearby locations on the standard obstacle-free map need to be considered for comparison.

Once a matching pair is identified, the discrepancy $Z$ between the road position corresponding to the real-time image and that of the matched standard road image is determined as the first parameter for alignment. The specific meaning of $Z$ is as follows: If $Z = 0$, it indicates that the standard road image, which is at the exact location as the real-time image, is the optimal match. If $Z = 1$, it signifies that the next standard road image, corresponding to the road position in the real-time image, has been selected as the optimal match. The next step involves aligning the collected real-time image with the corresponding standard information by adjustments such as rotation and translation. This study employs the Homography transformation to process the real-time images. The corresponding points in the images from different viewpoints—that is, the real-time image and the standard obstacle-free road image—are related as follows:

$$\begin{bmatrix} x_1' \\ y_1' \\ 1 \end{bmatrix} = H \begin{bmatrix} x_1 \\ y_1 \\ 1 \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} & h_{13} \\ h_{21} & h_{22} & h_{23} \\ h_{31} & h_{32} & h_{33} \end{bmatrix} \begin{bmatrix} x_1 \\ y_1 \\ 1 \end{bmatrix} \tag{66}$$

In this calibration method, $[x_1 \quad y_1 \quad 1]^T$ and $[x_1' \quad y_1' \quad 1]^T$ represent the homogeneous coordinates of the original and transformed pixels, respectively. The matrix $H$ is the homography matrix that needs to be determined. To circumvent the effects introduced by obstacles, the Random Sample Consensus (RANSAC) algorithm (Chum &

Matas, 2008) is applied to select the feature matching points between the real-time image and the standard road image. By running the RANSAC algorithm multiple times, matching points are filtered from the multitude of matching features, and the H matrix is calculated. This iteration continues until the optimal H matrix is determined. At this point, this H matrix, along with the previously determined road position offset Z, is applied to other real-time road images. If it successfully identifies the corresponding standard road information image, then the image alignment and calibration phase is considered complete. If the road conditions are good and cumulative errors are not significant, verification can be conducted during the first pass by the high-speed data storage station after each departure. If the errors are substantial, calibration may need to occur each time the train passes near the station.

**Maximizing the Use of All Available Information**

The greatest advantage of the obstacle detection method based on differences proposed in this study is its sensitivity and computation speed. However, the difference processing can result in a loss of absolute color accuracy from the original images, leading to potential inaccuracies in classifying obstacles with existing image target recognition algorithms. To fully utilize the original information, this research introduces a real-time analysis and dual-track decision-making information fusion strategy.

Considering that the original real-time road information target recognition operates slowly, while the simplified obstacle detection is much faster, this method intersperses the results of the original road information target recognition into the results of the simplified obstacle recognition based on their computation speed ratio. In other words, the input to the subsequent automatic deceleration decision system consists of a continuous series of refined obstacle detection images interspersed with results from the original image detection. This information fusion system increases the frequency of information transfer and enhances the density of the information while preserving the accuracy of the detection process (Clouqueur, Ramanathan, Saluja, & Wang, 2001; Dasarathy, 1994).

## 6.5 Experiments

### 6.5.1 Preliminary Experiments

In this section, this research conducts experiments to verify the broad applicability of the approach and to demonstrate the superior performance of the CODS (Custom Obstacle Detection System).

**Preliminary Experiments with RGB images**

This chapter has established the efficacy of the CODS independently of the architecture of the target detection models and evaluation metrics used. In this experimental phase, this chapter incorporated the CODS paradigm into three widely-used target detection models based on RGB image information, maintaining the hyperparameter settings as per their original designs. The results are presented in Table 24. It is particularly noteworthy that the version of the target detection model selected for this phase of the experiment represents the optimal model trained by the original teams of these algorithms. The involved target detection models were not retrained using the collected comparative datasets. Therefore, in this experimental stage, the enhancement provided by the CODS is in a plug-and-play form, eliminating the need for additional configurations.

As shown in Table 24, compared to baseline models, integrating CODS significantly enhances the accuracy and computational speed of various object detection models. These results indicate that CODS is a versatile method, applicable to other object detection frameworks. Particularly notable is the improvement in the IoU metric, where CODS effectively filters out irrelevant information, resulting in more precise boundary details of prediction boxes, achieving an enhancement ranging from a minimum of 2% to a maximum of 33%.

Furthermore, the results reveal a marked improvement in detection speed, especially notable in Yolov8, where the total processing time is nearly halved. This is because CODS substantially reduces the information load of the original images, reducing unnecessary calculations. Interestingly, as the DETR model heavily relies on the correlation between local and surrounding environmental information, with the addition of CODS, its Average Precision (AP) remains stable or slightly decreases. This unexpectedly underscores the significance of the DETR approach. For future research, balancing the preservation of

some environmental information by CODS to enhance the accuracy of the DETR model, while maintaining a balance between speed and accuracy, presents a novel challenge.

Qualitative results are shown in Figure 33. From the figure, it is evident that after processing by the CODS system, information related to the environmental background is effectively filtered out, leaving key obstacle-related information that can be efficiently utilized by other object detection models. This aids the object detection models in more acutely recognizing previously undetectable objects, such as the signpost in a nighttime scene in the second column of Figure 33, and the car emerging from a crossroad in a heavy rain scenario in the third column.

Table 24. Quantitative analysis of obstacle detection.

| Model | Average Precision | | | | mIoU | | | | FPS |
|---|---|---|---|---|---|---|---|---|---|
| | $AP_{Car}$ | $AP_{People}$ | $AP_{Irregular}$ | mAP | Car | People | Irregular | All | Average |
| YoloV8 | 86.23 | 83.51 | 34.87 | 70.01 | 75.63 | 70.53 | 51.39 | 66.83 | 22.04 |
| YoloV8+CODS | **87.26** | **85.46** | **50.29** | **75.63** | **79.25** | **73.31** | **68.21** | **74.16** | **38.57** |
| Δ AP/mIoU/FPS | +1.03 | +1.95 | +15.42 | +5.62 | +3.62 | +2.78 | +16.82 | +7.33 | +16.53 |
| Faster R-CNN | 87.25 | 85.37 | 45.79 | 74.25 | 65.48 | 67.82 | 59.61 | 64.42 | 8.82 |
| Faster R-CNN+CODS | **89.31** | **87.42** | **52.37** | **77.66** | **71.54** | **69.42** | **73.94** | **71.62** | **11.37** |
| Δ AP/mIoU/FPS | +2.06 | +2.05 | +6.58 | +3.41 | +6.06 | +1.6 | +14.33 | +7.2 | +2.55 |
| DETR | 83.42 | 82.93 | 37.26 | 69.43 | 71.25 | 73.62 | 58.84 | 68.24 | 9.64 |
| DETR+CODS | **84.61** | **81.49** | **45.62** | **71.98** | **75.87** | **78.91** | **72.63** | **75.81** | **9.81** |
| Δ AP/mIoU/FPS | +1.19 | -1.44 | +8.36 | +2.55 | +4.62 | +5.29 | +13.79 | +7.57 | +0.17 |

Note: Performance of the target detection algorithm methods and their versions augmented by CODS on the Carla validation set. CODS continuously improves these methods by adding customized criterion information.

**Preliminary Experiments with LiDAR point cloud data**

In the experiments involving the processing of 3D point cloud data, the CODS (Custom Obstacle Detection System) algorithm's results were significantly superior to those of traditional point cloud segmentation algorithms, which negated the need to combine traditional segmentation techniques with the CODS approach. Thus, this study compares the obstacle segmentation outcomes of the CODS directly with three segmentation algorithms based on 3D point cloud information. The results are documented in Table 25, with qualitative outcomes depicted in Figure 34.

Table 25. Quantitative analysis of point cloud segmentation performance.

| Model | mIoU | FPS |
|---|---|---|
| DBSCAN | 57.12 | 70.2 |
| RANSAC | 16.48 | 21.1 |
| PointNet | 65.31 | 8.6 |
| CODS | **96.81** | **116.3** |

Note: The mIoU values presented in the table are exclusively related to obstacle segmentation and do not include results pertaining to the background segmentation. By adding standard road data through, CODS achieves significantly higher segmentation efficiency and accuracy than conventional algorithms.

The results indicate that the CODS can accurately segment inconsistencies within standard road information in an exceptionally short timeframe. The RANSAC algorithm, owing to its strong randomness, struggles to achieve consistently superior results across tests with a fixed set of hyperparameters. While it demonstrates certain advantages in segmentations that include background elements like buildings, its performance is less satisfactory in obstacle-only segmentations, as shown in Table 25. Both DBSCAN and PointNet effectively segment obstacles, with PointNet exhibiting the capability to partially segment obstacles closely intertwined with background information, showcasing the feature extraction ability of CNN networks. However, as PointNet incorporates neural network structures, its computational speed is not comparable to purely numerical segmentation algorithms. Notably, CODS, due to its segmentation process that avoids

loops and allows for parallel processing, significantly enhances computational speed. Furthermore, compared to traditional point cloud segmentation algorithms, the processing speed of the CODS has significantly surpassed the data collection rate. In other words, the CODS is capable of real-time processing of fused data streams from multiple LiDAR sensors. This represents a significant breakthrough.

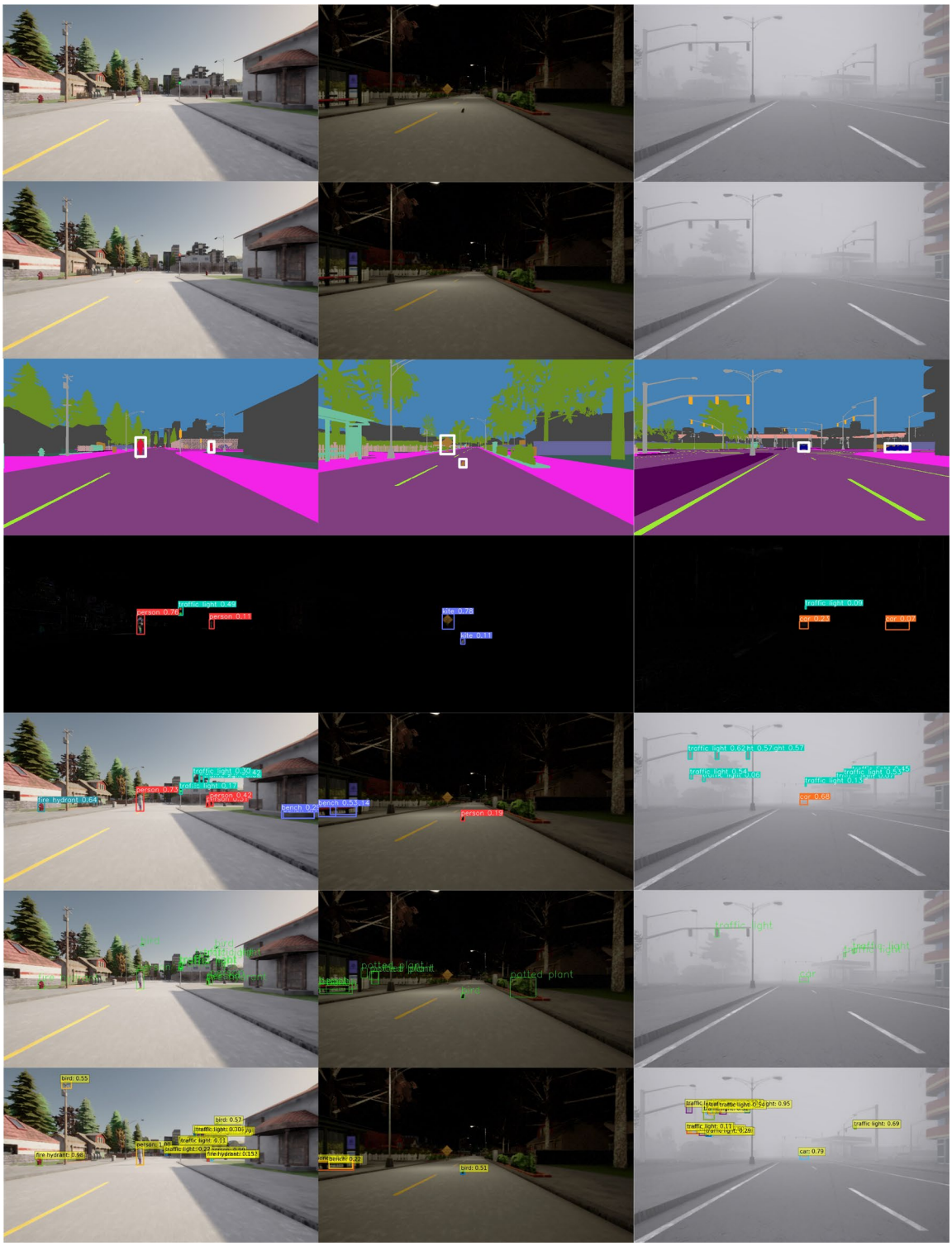


*Figure 33. The Qualitative analysis of CODS's effectiveness.*

Note: The rows, from top to bottom, represent: real-time recorded road conditions, unobstructed standard road maps, accurate semantic segmentation images generated directly by the CARLA system (ground truth), detection results of the YOLO model

enhanced by CODS, and comparisons with YOLO model, Faster R-CNN, and DETR. The columns, from left to right, correspond to: normal scenarios, nighttime scenes, and heavy rain conditions. It is apparent that CODS effectively filters out background information, assisting detection models in ignoring irrelevant data and identifying obstacles that were previously undetectable.

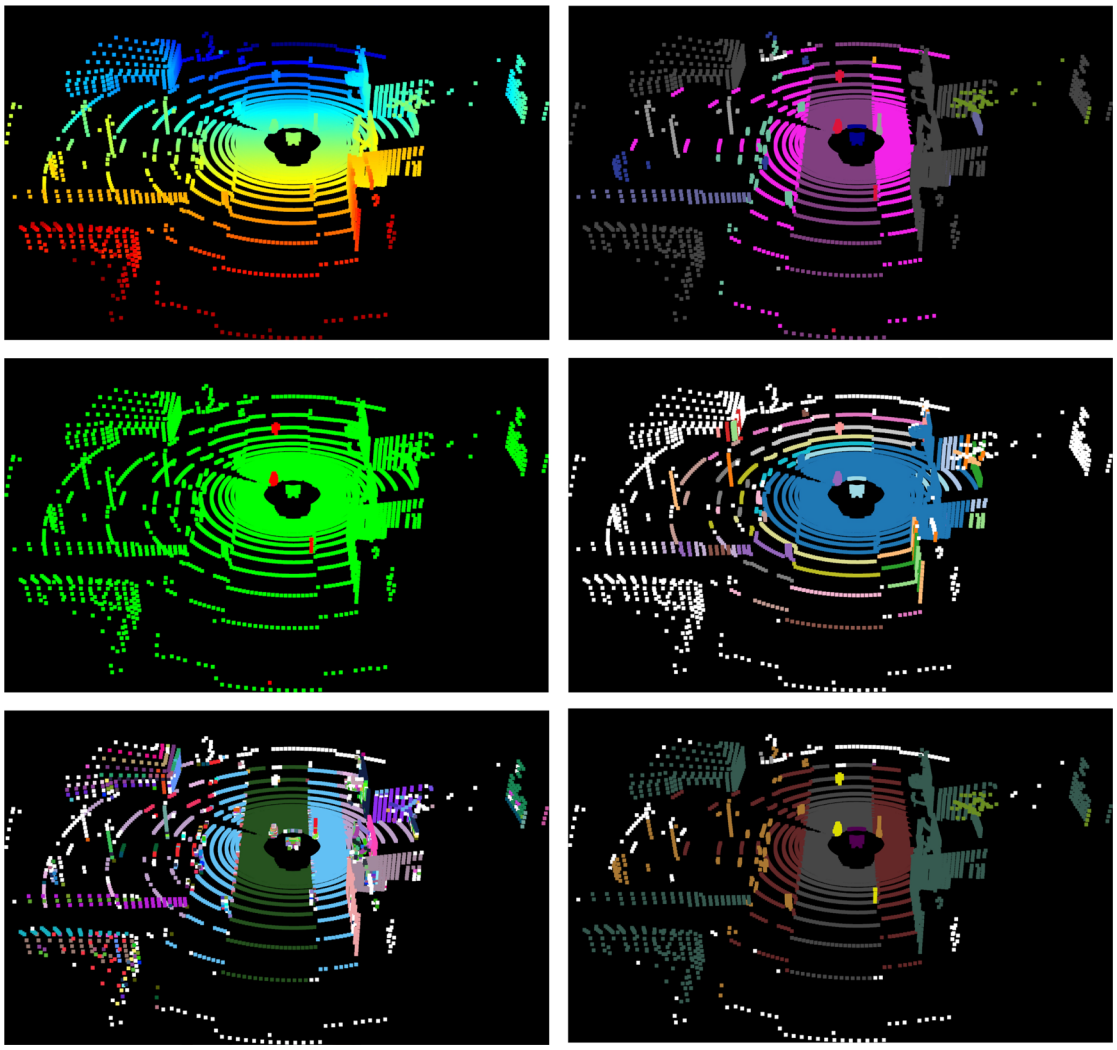


*Figure 34. Qualitative analysis of the effectiveness of CODS in LIDAR data.*

Note: The six diagrams are: (1) Real-time recorded road conditions, (2) Accurate LIDAR semantic segmentation images generated directly by the CARLA system (ground truth), (3) Segmentation results of CODS, (4) DBSCAN, (5) RANSAC, (6) PointNet. The point cloud diagrams depict the same location and scene as the first

column of Figure 33. In images (4), (5), and (6), the white point clouds represent points that have not been segmented.

### 6.5.2 Maximum Braking Distance

Given that the maximum detection range and data acquisition speed of LiDAR significantly lag behind those of RGB cameras, this phase of the experiment focuses solely on the Maximum Braking Distance (MBD) differences under the information collected by RGB cameras. The best-performing YOLOv8 model from the previous phase was selected for comparison. The experiment contrasted the MBD for different types of objects and angles with and without the enhancement of CODS.

The CODS incorporates critical road information beyond the line of sight, which significantly aids the identification system in detecting objects that are further away, smaller, and uncommon. This, in turn, is beneficial for navigation, planning, and decision-making processes. To substantiate the enhancements brought about by CODS, this chapter articulated the scope of obstacle detection using the standard of Maximum Braking Distance. The specific experiments included common traffic participants: vehicles, motorcycles, and pedestrians; traffic signal indicators: signs and traffic cones; and the most challenging category—minute objects: irregular-shaped washers and garbage bottles. To escalate the challenge, the study also involved downsizing the obstacles and altering the perspectives to compel the obstacle detection system to recognize the presence of obstacles with as little information as possible. Table 26 consistently demonstrates improved detection outcomes across standard views, side views, reduced sizes, and combinations of side views and reductions. The results are presented in Table 26.

Table 26. Performance of the furthest braking distance in different viewing situations.

| Level of Difficulty | + CODS | Furthest Braking Distance | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Traffic participants | | | Signal | | Small | |
| | | Car | Motorbike | People | Signposts | Barricade | Irregular | Rubbish |
| Normal | × | 61 | 34 | 32 | 26 | 18 | 1 | 3 |
| | √ | **68** | **37** | **35** | **27** | **23** | **3** | **6** |
| Δ Distance: meter(percent) | | +7(11%) | +3(9%) | +3(9%) | +1(4%) | +5(28%) | +2(200%) | +3(100%) |
| Side view | × | 63 | 39 | 31 | 24 | 18 | 1 | 3 |
| | √ | **69** | **41** | **34** | **26** | **23** | **3** | **5** |
| Δ Distance: meter(percent) | | +6(10%) | +2(5%) | +3(10%) | +2(8%) | +5(28%) | +2(200%) | +2(67%) |
| Smaller | × | 46 | 25 | 23 | 19 | 14 | 1 | 2 |
| | √ | **51** | **28** | **25** | **20** | **18** | **2** | **3** |
| Δ Distance: meter(percent) | | +5(11%) | +3(12%) | +2(9%) | +1(5%) | +4(29%) | +1(100%) | +1(50%) |
| Side and Smaller | × | 47 | 27 | 22 | 17 | 14 | 1 | 1 |
| | √ | **51** | **29** | **24** | **19** | **18** | **2** | **2** |
| Δ Distance: meter(percent) | | +4(9%) | +2(7%) | +2(9%) | +2(12%) | +4(29%) | +1(100%) | +1(100%) |

The experimental outcomes reveal that with the assistance of CODS, the obstacle recognition system can detect obstacles at greater distances. It is noteworthy that, in scenarios involving smaller-scale and irregularly shaped obstacles, the integration of CODS significantly enhances the YOLO model's ability to recognize obstacle targets. This enhancement results in a substantial increase in detection distance, particularly when the original distance base is small. This implies that in high-speed railway scenarios, a detection system augmented with CODS can identify potential obstacles earlier, even when they occupy a minimal area in the field of vision (indicating a significant distance), thereby allowing for earlier deceleration and reducing potential harm. Additionally, for obstacles like barricades, which are easily misled by background environments and have limited representation in the training datasets of detection models, CODS greatly assists in increasing the effective recognition distance. While it may not categorize barricades into the correct class with certainty, it can detect their presence in a timely manner.

Table 27. Performance in adverse weather conditions

| Environment | + CODS | Average Precision | | | |
|---|---|---|---|---|---|
| | | $AP_{Car}$ | $AP_{People}$ | $AP_{Irregular}$ | mAP |
| Normal | × | 86.23 | 83.51 | 34.87 | 70.01 |
| | √ | **87.26** | **85.46** | **50.29** | **75.63** |
| Δ AP/mIoU | | +1.03 | +1.95 | +15.42 | +5.62 |
| Night | × | 65.12 | 45.21 | 15.36 | 44.22 |
| | √ | **68.63** | **56.47** | **23.86** | **51.55** |
| Δ AP/mIoU | | +3.51 | +11.26 | +8.5 | +7.33 |
| Rain | × | 30.26 | 28.31 | 0 | 20.60 |
| | √ | **47.62** | **43.89** | **10.34** | **35.32** |
| Δ AP/mIoU | | +17.36 | +15.58 | +10.34 | +14.72 |
| RainNight | × | 10.38 | 5.49 | 0 | 5.80 |
| | √ | **20.62** | **10.56** | **6.43** | **13.35** |
| Δ AP/mIoU | | +10.24 | +5.07 | +6.43 | +7.55 |

### 6.5.3 Performance Under Adverse Weather Conditions

Obstacle detection systems face significant challenges under adverse weather conditions or in situations of poor lighting, such as during rain or at night, which can impede the accurate identification of road information. Nevertheless, the Custom Obstacle Detection System (CODS) algorithm is adept at filtering out and retaining the most salient features of obstacles, thus providing enhanced reliable information for vehicles to precisely perceive obstacles in their path during the current journey.

As demonstrated in Table 27, the application of CODS leads to greater improvements under challenging conditions, such as rain and nighttime, compared to normal weather scenarios. This indicates that the obstacle detection system effectively leverages the necessary role of standard road information under the corresponding environmental conditions.

### 6.5.4 Limitations of the Case

Despite the considerable advancements demonstrated by Customized Obstacle Detection System (CODS) for high-speed railway applications, there are inherent limitations that currently constrain its broader applicability. Firstly, the system's dependency on the alignment between the standard obstacle-free rail information and the real-time data collection presents a notable challenge. This alignment issue restricts the usage of CODS primarily to railway scenarios where the route is fixed and the perspective changes are minimal. The current model has not been optimized for the dynamic and multifaceted environments encountered in autonomous driving systems for automobiles. CODS is, therefore, not yet equipped to handle the collaborative multi-lane information, high-frequency map updates, and the impact of vehicular movements that are requisite for such systems. Secondly, certain environmental factors, such as weather variations that introduce interference like rain, cannot be efficiently accounted for in the standard map. These dynamic changes are challenging to incorporate in real-time within the predefined framework, leading to potential lapses in the detection capability of the system under certain adverse conditions. Although integrating existing mature object detection models represents the most straightforward approach, it must be acknowledged that the training

data for these established models differs from differential image data. This discrepancy can lead to reduced accuracy under specific circumstances.

### 6.5.5 Future Perspectives of the Case

Looking ahead, the research trajectory is firmly directed toward overcoming the aforementioned limitations and further enhancing the CODS framework's precision and speed. One pivotal area of development will involve advancing the system's capability to seamlessly integrate and align real-time data with the existing map information. This improvement is crucial for expanding the system's applicability beyond rail transportation to autonomous vehicular systems, where the environmental and perspective changes are more pronounced and unpredictable.

Additionally, the robustness of the system against environmental influences, such as adverse weather conditions, is another critical facet that requires substantial enhancement. Future iterations of the system will integrate more sophisticated sensors and algorithms capable of distinguishing genuine obstacles from transient environmental effects.

To address the disparities arising from the dataset and enhance the upper limit of the detection model's capabilities, the next phase of the project will involve the modification of established object detection algorithms. This will entail simplifying redundant computations within the model framework using refined data, and further training the object detection models using an expanded collection of differential datasets.

In parallel, efforts will be concentrated on optimizing data storage and transmission processes. By implementing more efficient data compression algorithms and developing smarter storage solutions, this research aims to significantly reduce the spatial and bandwidth requirements for map data handling. This evolution will not only economize on resource usage but also facilitate quicker system responses, contributing to safer and more reliable high-speed rail operations.

Collectively, these advancements are expected to not only refine CODS but also contribute broadly to the field of intelligent transportation systems, reinforcing the foundations for safer, more efficient, and intelligent high-speed rail technologies.

### 6.5.6 Conclusion and Discussion of the Case

This study has embarked on an ambitious journey to address the critical challenge of real-time obstacle detection in railway systems, a domain where safety and efficiency are paramount. Through a meticulous synthesis of sensor data and advanced computational techniques, this chapter has developed a robust framework that not only detects but also anticipates potential hazards on railway tracks with unprecedented accuracy.

The research has culminated in the creation of a "Customized Obstacle Detection System (CODS)", which stands as a testament to the innovative integration of standard obstacle-free maps and real-time detection capabilities. The system's architecture, which harnesses the synergy of RGB cameras and LiDAR sensors, has been designed with the dual objectives of adaptability and precision in mind. The empirical evidence, as presented in the preceding sections, underscores the system's proficiency in navigating the complex tapestry of railway environments.

The experimental validation, conducted within the Carla simulation environment, has yielded promising results, demonstrating a 10% increase in detection mean average precision and a maximum improvement of 75% in detection speed. The performance in point cloud data was even more stunning, achieving the absolute leading score with an almost perfect pairwise accuracy of over 96 and a speed of over 116fps.These figures are not merely statistical triumphs but represent significant strides towards enhancing the safety protocols in high-speed railway operations. The use of evaluation metrics such as Mean Intersection over Union (mIoU), Mean Average Precision (mAP), and the novel Maximum Braking Distance (MBD) has provided a comprehensive assessment of the system's performance, ensuring that the findings are grounded in a rigorous analytical framework.

Moreover, the CODS framework's ability to discern and adapt to the dynamic nature of railway settings has been proven through its self-supervised map updates and distributed storage mechanisms. The application of algorithms like SIFT and KNN has further fortified the system's analytical prowess, enabling it to distinguish between standard environmental changes and genuine obstructions with a high degree of reliability, ensuring rigour in map updating.

In conclusion, the research presented herein not only paves the way for a new era of

railway safety technology but also opens up a plethora of opportunities for future enhancements. The CODS framework, with its proven scalability and adaptability, is poised to be integrated into existing railway infrastructures seamlessly. As we look towards the horizon, it is clear that the methodologies and technologies developed in this study will have a lasting impact on the trajectory of railway transportation research and technology, steering it towards a future where travel by train is as safe as it is swift.

The implications of this research are far-reaching, extending beyond the confines of academic discourse and into the realm of practical, on-the-ground applications that could save lives and safeguard property. It is our hope that this study will serve as a catalyst for further innovation in the field, inspiring continued exploration into the vast potential of intelligent transportation systems.

## 6.6 Proof of the Principle

**Introduction to the Landauer Limit**

The Landauer Principle (Ribezzi-Crivellari & Ritort, 2019; Tobin & Blackledge, 2014), introduced by Rolf Landauer in 1961, posits a fundamental limit on the minimum amount of energy required to erase one bit of information, quantified as $kT\ln(2)$ joules, where $k$ is the Boltzmann constant ($1.380649 \times 10^{-23}\text{J/K}$) and $T$ is the temperature of the computational device in kelvins. This principle highlights the intrinsic physical cost of information processing, establishing a theoretical baseline for the energy efficiency of computational operations. The principle is mathematically represented as:

$$E = kT\ln(2) \tag{67}$$

**Efficiency in Information Utilization**

Efficiency in information utilization within ML models, particularly those inspired by core characteristics of specific scenarios, can be mathematically framed through information theory metrics such as entropy (H) and mutual information (I).

Entropy, a measure of the unpredictability or randomness of information content, is defined for a discrete random variable $X$ with possible values $\{x_1, x_2, \ldots, x_n\}$ and probability mass function $P(X)$ as:

$$H(X) = -\sum_{i=1}^{n} P(x_i)\log_2 P(x_i) \tag{68}$$

Mutual information between two random variables X (input features) and Y (target variable) quantifies the amount of information obtained about one through the other. It is defined as:

$$I(X;Y) = \sum_{y\in Y}\sum_{x\in X} p(x,y)\log_2\left(\frac{p(x,y)}{p(x)p(y)}\right) \quad (69)$$

Focusing on core characteristics aligns with optimizing mutual information, ensuring that the model prioritizes features (X) that provide the maximum predictive power about the outcome (Y), thus enhancing efficiency.

**Landauer Limit and Information Erasure**

The Landauer Limit conceptually ties to ML efficiency in the context of updating model weights during learning, especially when incorrect predictions are "erased" or corrected. In an ideal scenario, this correction process should be as energy-efficient as possible, aligning with the minimal energy expenditure delineated by the Landauer Principle.

For an ML model adjusting its weights, the entropy change ($\Delta H$) associated with learning from an incorrect to a correct state, for a binary classification, could be simplified and conceptualized as akin to a bit erasure, highlighting the energy-efficiency parallel:

$$\Delta H = H_{initial} - H_{final} \quad (70)$$

Assuming $H_{initial}$ is the entropy with an incorrect prediction and $H_{final}$ is lower, reflecting a state of higher certainty post-correction.

Incorporating the Landauer Limit into the efficiency analysis of ML models, this research aims to minimize the computational "energy" (or analogously, the computational resources) needed for processing and updating information. This is achieved by:

Reducing Entropy. Prioritizing core characteristics leads to a reduction in the model's entropy, implying a more ordered state of information and, consequently, more energy-efficient processing.

Maximizing Mutual Information. Enhancing the mutual information between input features and the target variable ensures that the model's updates are highly informative and directly contribute to improving predictions, akin to an energy-efficient "information

erasure" process where corrections are made with minimal waste.

The mathematical exploration of efficiency in information utilization within ML models, inspired by core characteristics and analyzed through the lens of the Landauer Limit, unveils a profound intersection between computational information theory and physical principles governing energy expenditure. By striving for maximal mutual information and minimal entropy within model data processing, this chapter tries to align the operational efficiency of ML models with the fundamental limits of physical laws, marking a step towards not only more accurate and interpretable models but also toward realizing the vision of sustainable and energy-efficient computational intelligence. This synthesis of computational efficiency and physical energy constraints not only provides a richer understanding of the theoretical underpinnings of ML model design but also opens pathways to novel approaches that respect both the complexity of data and the finite nature of our physical resources.

## 6.7 Summary

In the realm of Machine Learning Models Inspired by Core Characteristics of Special Scenarios, the study has embarked on a transformative journey, culminating in the development of the Customized Obstacle Detection System (CODS) for high-speed railway systems. This endeavor underscores a pivotal shift towards leveraging the unique aspects of specific scenarios to substantially elevate the performance and applicability of machine learning models. The enhancements brought about by the approach are multifaceted, extending across the realms of precision, speed, and interpretability, which are critical for the deployment in environments where safety and efficiency are paramount. The Customized Obstacle Detection System (CODS), a pioneering framework that synergizes real-time sensor data with pre-established obstacle-free maps to markedly enhance detection accuracy and speed. This section synthesizes the core findings, delineates the methodological innovations introduced, and elucidates the broader implications of the research.

**Innovations and Contributions**

1. Enhanced Obstacle Detection. CODS, leveraging scenario-specific characteristics and sophisticated data integration, has achieved a notable 10% uplift in detection mean average precision, alongside a 75% enhancement in processing velocity, setting a new benchmark for obstacle detection in railway systems.

2. Advanced Feature Engineering. Through the meticulous harnessing of domain-specific features, the approach has not only heightened model performance but also adeptly navigated the challenges of data skewness, enabling more nuanced distinction capabilities.

3. Model Interpretability and Adaptability. By embedding scenario-specific insights into the model architecture, CODS has not only improved interpretability but also furnished the model with the capacity to adjust dynamically to evolving environmental conditions, a crucial advancement for sustained model efficacy.

This chapter presents a new framework, as shown in Figure 35. Unlike the previous two chapters, there are no individual objects in this scenario that require special attention, so no targeted enhancements are made to a specific one. The grey part shown in this framework is the process of traditional obstacle detection, and the yellow part is the additional tasks inspired by the core characteristics of the scenario proposed in this chapter.

**Addressing Core Challenges**

By intricately mapping the nuanced distinctions within data, particularly leveraging obstacle-free maps and sensor inputs, CODS has significantly bolstered detection precision, Recognized subtle differences. A skillful data differencing scheme that directly identifies obstacles by doing the difference, transforming complex problems into common ones, tailored to simulate rare scenarios within high-speed rail contexts, has effectively combated data imbalances, enhancing model robustness and minority sample discrimination. Design the algorithmic process in a way that is consistent with human intuition. The integration of intuitive, scenario-specific elements into the model design has rendered the decision-making process more transparent and trustworthy. Enhancement of Adaptive Capabilities. CODS's dynamic updating mechanism, which refines obstacle-free maps with real-time

data, ensures enduring model performance amidst environmental changes.

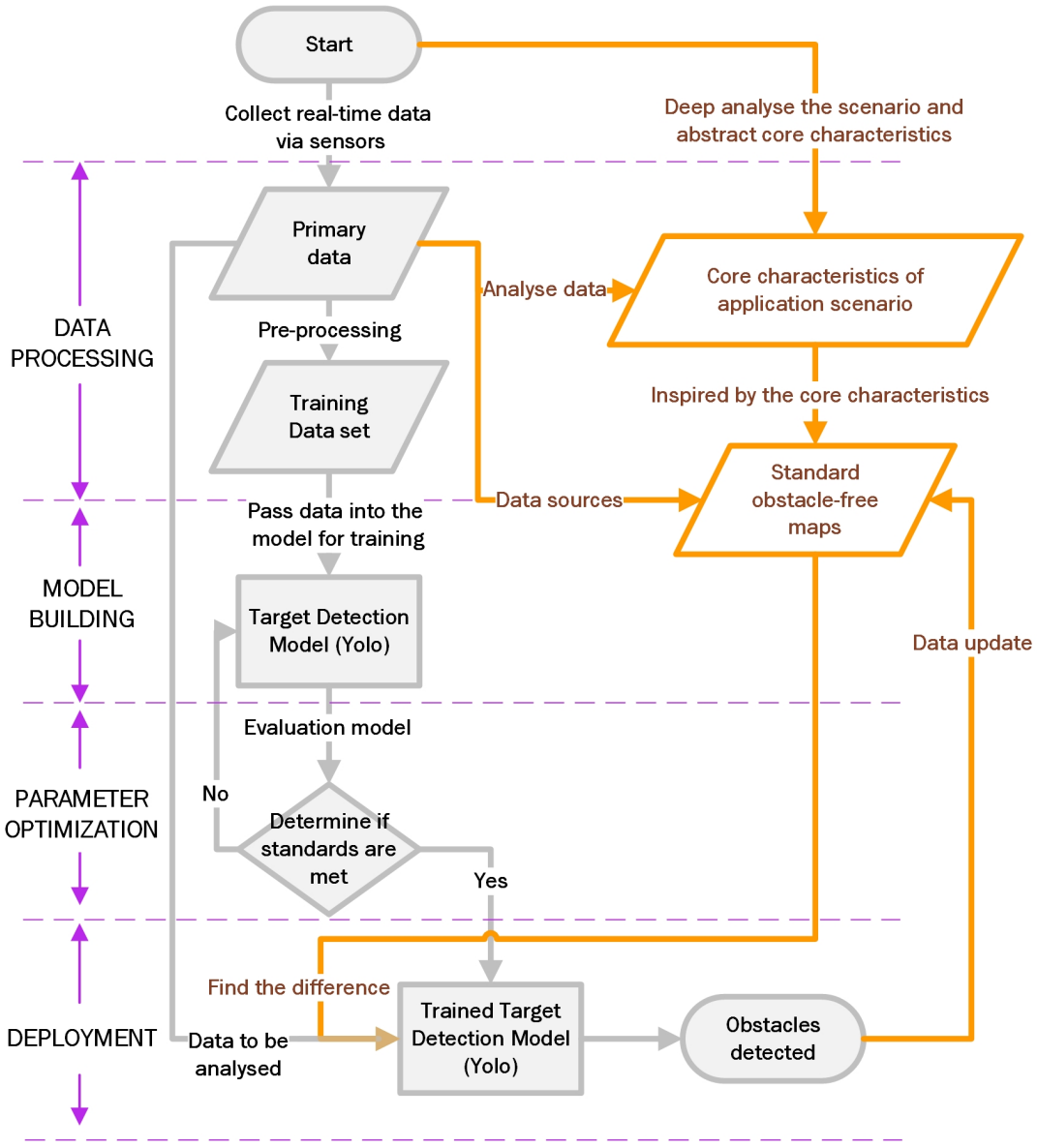



*Figure 35. Flowchart for obstacle detection optimization inspired by core characteristics of the scenario.*

**Future Directions**

The achievements of this study not only signify a leap forward for ML applications in high-speed railways but also herald new horizons across various domains. The success of CODS underscores its potential expansibility to other intelligent transportation arenas, promising notable gains in safety and efficiency. These findings advocate for a fusion of domain expertise with computational innovation, a synergy that can propel the

development of scenario-specific ML models to new heights. Continued Innovation. Future research will refine the CODS framework, particularly its data integration capabilities, and explore its adaptability to a broader spectrum of operational environments.

In conclusion, the journey through the development and application of machine learning models inspired by core characteristics of special scenarios has revealed the untapped potential of customized approaches in enhancing model performance. As we move forward, the insights gained from this study will serve as a cornerstone for future explorations, driving innovations that are tailored to meet the unique demands of various applications, and paving the way for the next generation of machine learning models that are more precise, interpretable, and adaptable.

*Transition Paragraph: Chapter six elevates scenario-based machine learning to a higher dimension for scenario analysis, achieving impressive results that are both efficient and precise. Thus, chapters four, five, and six have detailed the practical implementation and application of scenario -based machine learning. In the final chapter, we will discuss the coordination of the entire project and some of the significant achievements realized.*

# CHAPTER 7 CONCLUSIONS

The machine learning algorithms that are widely used nowadays are the products of repeated iterative upgrades with a considerable degree of advantage over the past decade. This study provides a comprehensive analysis of the available machine learning models and a preliminary discussion of their customization for scenarios. From the conclusions drawn so far, SCENARIO-BASED MACHINE LEARNING MODELS have obvious advantages and are worthy of continued in-depth study with a view to form more complete algorithms for industrial adoptions.

## 7.1 Research Outcomes

The thesis addresses critical challenges in the machine learning domain, emphasizing the transition from universal, general-purpose models to scenario-specific, customizable models. This approach marks a significant paradigm shift, prioritizing adaptability, lightweight designs, and precision over the conventional machine learning model's quest for universality and generalized accuracy. The main findings and contributions of this research encapsulate a novel perspective on machine learning model development. By introducing a framework that defies the traditional "impossible trinity" of machine learning—universality, lightweight, and accuracy—the study demonstrates that models tailored to individual entities or specific scenarios can achieve higher accuracy and efficiency.

The thesis makes a compelling case for the importance of scenario-specific information in enhancing the performance of machine learning models. Through detailed experiments and comparative analyzes, it has been shown that by catering specifically to individual entities, considering the target objects and the correlations among individuals, and leveraging scenario-related information, machine learning models can achieve remarkable results. For instance, a customized approach in a Hepatitis C dataset achieved a notable accuracy improvement, and the application of scenario-based customization in large-scale heart disease screening scenarios demonstrated efficacy in model lightweight and real-time updates, thus enhancing privacy protection and efficient data utilization.

Furthermore, by exploring the core characteristics of specific scenarios, such as obstacle detection in high-speed railways, the research illustrates the feasibility of dramatically improving model performance through scenario-based customization. The introduction of the Customized Obstacle Detection System (CODS) showcases a tangible application where scenario-based models significantly outperform traditional approaches in accuracy and operational speed.

These results clearly illustrate how this research fills the gaps in existing research by challenging the blind pursuit of "general-purpose" metrics and expanding the current body of knowledge on machine learning, which is difficult to customize, make full use of the data, balance efficiency and accuracy, and be easy to use by individual users. This research not only provides a theoretical framework for developing scenario-based machine learning models, but also validates this approach through real-world applications, thus providing a new direction for future research in this area.

In conclusion, this doctoral thesis presents a groundbreaking approach to machine learning, emphasizing the significance of customization and scenario-specific design. By diverging from the path of seeking universality and general-purpose models, it opens new avenues for research and application in machine learning, promising more efficient, accurate, and user-friendly models tailored to specific needs and scenarios. This work significantly contributes to the literature, offering fresh insights and practical solutions to the challenges facing machine learning development today.

## 7.2 Systematic Use of Scenario-Based Machine Learning

Chapters four, five, and six individually introduced machine learning models tailored to a single individual object, based on the specific requirements of the application scenario, and inspired by core characteristics of special scenarios. This section summarizes how to systematically utilize scenario-based machine learning.

First, the ideas presented in the previous three chapters are distilled through a keyword for each:

Tailored to a single individual object: **Focus**

Based on the specific requirements of the application scenario: **Around**

Inspired by the core characteristic of special scenarios: **Abstract**

Traditional machine learning starts with data, training models from this data to solve problems, following the sequence “data -> model -> problem”.

In contrast, scenario-based machine learning begins with the problem, viewing the data through the lens of this problem. It involves a meticulous examination of each object to be analyzed (**Focus**); after fully understanding the relationship between the problem and the data, the problem is embedded into application scenarios, collecting, analyzing, and summarizing information and standards not covered by the dataset (**Around**); the information gathered is then synthesized, simplifying complex issues to uncover the core commonalities of the problem (**Abstract**). By focusing on the core of the problem, while considering the requirements of the scenario and paying attention to individual objects, models are designed and trained to ultimately solve the problem.

This thesis demonstrates a full process of “problem -> data -> model -> problem,” but this unique approach also imposes higher demands on researchers and practitioners of machine learning. Firstly, attention to individual entities should be based on a people-centric philosophy, not sacrificing the predictive accuracy for specific individuals for the sake of improving overall dataset performance. Additionally, it requires a commitment to optimizing for specific, challenging corner cases. More demanding still is the need to adopt a multi-objective optimization mindset, bringing the problem into real-world scenarios for comprehensive consideration. This demands that practitioners not confine themselves to the original confines of datasets but instead step out into the field to truly understand the specific problems that algorithms are meant to solve. Lastly, abstracting the problem is a lifelong pursuit for engineering professionals. Accurately identifying and fully utilizing “first principles” is the key to ingeniously solving problems.

## 7.3 Reviewing the Problem Statement and Objectives

It is time to examine the problem that this research is trying to solve and the objectives as stated in section 1.3 of the thesis. The answers to the stated questions are as follows:

*1) How to build a model that can meet the needs of various scenarios by adjusting hyper-parameters?*

Answer: It is impractical to expect that adjusting hyper-parameters alone will meet the needs of all scenarios. While hyper-parameter tuning can facilitate model transfer or optimization in similar contexts, it often falls short when significant changes in scenarios occur. In such cases, the performance of the model in new scenarios cannot be guaranteed through mere hyper-parameter adjustments. Instead, a systematic solution must be derived from the actual conditions of the new scenario, tailored specifically to that context, and following the scenario-based framework.

*2) How to create a lightweight but still high-accuracy model?*

Answer: Starting from the specific scenario, simplify the problem by focusing on its core characteristics. Additionally, consider the comprehensive information related to the scenario to achieve a balance among multiple target parameters. Then, enhance accuracy by customizing models for the individual objects within the scenario.

*3) How to iterate the machine learning model quickly in the face of the rapidly updated data?*

Answer: Systematic solutions formulated based on a scenario-based framework can greatly simplify and accelerate the training process and optimize model updating strategies. This allows the model to utilize data to achieve nearly real-time updates.

*4) How to achieve full utilization of the collected data with a focus?*

Answer: Systematic solutions developed within a scenario-based framework can effectively integrate data with the scenario, leveraging the core characteristics of the scenario to discern the significance of multi-dimensional and multimodal data. This approach also involves analyzing the correlations between an individual object's data and other information, enabling focused use of data within specific objects.

**In light of the several issues and specific tasks raised above, the objectives of the project are trifold and summarized as follows:**

***1) Use scenarios-related prior knowledge to develop new models and algorithms for***

***some specific problems instead of general-purpose models, which are rarely studied in previous literature.***

Achievement: Considering the critical need for high accuracy in medical issues and the special requirement for individual privacy protection, an algorithm customized for individual objects has been developed. This algorithm trains a separate model for each individual object, which cannot be used for other individual objects.

***2) To improve the accuracy and reliability of the model, based on considering the time and computation power consumed in training.***

Achievement: Taking into account the consumption of training and computational resources, the scenario-based customized solutions have achieved exceptionally high accuracy and reliability across various types of datasets.

***3) To apply the newly developed models and algorithms to some real industrial or medical cases.***

Achievement: The effectiveness of these approaches have been validated and has achieved excellent results on datasets related to medical and autonomous driving applications.

## 7.4 Innovations

### 7.4.1 Theoretical Contributions

This thesis has presented a novel framework for developing machine learning models that are tailored to specific scenarios, addressing the limitations of the current "one-size-fits-all" approach in machine learning. The research has fundamentally challenged and expanded the prevailing paradigms within the field, offering a new lens through which machine learning can be viewed and applied. Specifically, the theoretical contributions are:

Introduction of the Scenario-Based Machine Learning Framework. This research introduces a groundbreaking theoretical framework that emphasizes the importance of

adaptability, lightweight, and precision in machine learning models. By proposing a scenario-based approach, it challenges the existing “impossible trinity” of universality, lightweight, and accuracy, providing a new path for model development that prioritizes the specific needs and nuances of individual scenarios over generalized model applicability.

### 7.4.2 Methodological Contributions

**Chapter 4: Machine Learning Models Tailored to a Single Individual Object**

In the realm of computer science, particularly within the ambit of machine learning, this chapter presents an innovative pivot towards the customization of models for individual objects, underlined by a compelling exploration within the healthcare sector for diagnosing Hepatitis C. The essence of this work resides in its challenge to the status quo, venturing beyond the conventional one-size-fits-all model to embrace the complexity and individuality inherent in real-world data. Through targeted data augmentation, adaptive bias adjustment, and hyperparameter optimization tailored to the individual’s unique data profile, this research not only addresses but surmounts the hurdles of data imbalance, insufficient model accuracy, interpretability issues, and the exigencies of dynamic health states.

Significantly, the introduction of a machine learning framework that personalizes the model for each potential patient embodies a transformative step towards precision medicine. By acknowledging and intricately addressing the diversity among individual health profiles, the research meticulously mitigates the limitations that beset traditional machine learning approaches in healthcare diagnostics. This personalization does not merely elevate the model’s diagnostic precision; it redefines the landscape of healthcare by making strides towards treatment and diagnostics that are as unique as the individuals they aim to serve. Meanwhile, the research provides a detailed methodological roadmap for creating customized and lightweight machine learning models.

**Chapter 5: Machine Learning Models Based on the Specific Requirements of the Application Scenario**

This chapter presents a pioneering exploration into the customization of machine

learning models for specific application scenarios, with a focal point on large-scale heart disease screening. It delineates a methodology that transcends traditional machine learning approaches by emphasizing the significance of tailoring models to individual patient data. This customization facilitates the identification of heart disease with remarkable efficiency and accuracy, a feat unattainable by general-purpose models. The chapter introduces three critical innovations: targeted data augmentation, adaptive attention mechanisms, and a nuanced validation set formulation, each designed to optimize model performance for individual cases.

The application of these methods in heart disease screening illustrates their potential to significantly improve diagnostic precision. By incorporating individual patient data into the model training process, the chapter demonstrates an approach that not only enhances the model's sensitivity and specificity but also addresses ethical considerations by ensuring data privacy and security. Also, the rapid incorporation of physician knowledge and utilization of new data demonstrates the superiority of customization for requirements. This customization approach presents a scalable, adaptable framework that can easily integrate interdisciplinary knowledge, thereby offering a robust solution for large-scale screening challenges.

**Chapter 6: Machine Learning Models Inspired by Core Characteristic of Special Scenarios**

Chapter 6 represents a significant stride towards addressing the nuanced demands of high-speed railway systems through the lens of machine learning. It meticulously outlines a paradigm shift from traditional, often static, machine learning approaches towards a more dynamic, scenario-specific model that leverages the "Domain-Specific Core Characteristics." This innovative approach not only promises enhanced precision in identifying and responding to obstacles but also embodies a leap towards models that are both interpretative and adaptable to the continuously evolving data landscapes characteristic of real-world applications. Particularly, the development and implementation of the "Customized Obstacle Detection System" (CODS) signify a pivotal advancement in leveraging machine learning to ensure safety and efficiency in high-speed rail

transportation. By synthesizing real-time sensor data with pre-established obstacle-free maps, CODS sets a new benchmark in obstacle detection — showcasing significant improvements in accuracy and processing velocity. This study not only illuminates the path for advanced research in intelligent transportation systems but also heralds a new era of machine learning models that are finely tuned to the specific nuances of the environments they operate within.

### 7.4.3 Contributions to Bridging Research Gaps

Research gaps are presented in 2.6.

**Gap 1. The obsession with models with a huge number of parameters and a particularly wide range of applicability formed during the development of the field of machine learning has led to a bottleneck in the direction of development.**

Solution: This research introduces scenario-based machine learning, illustrating and proving the viability of specialized, custom models. These models offer significant advantages in terms of the number of parameters, paving new directions for scenario-based machine learning research.

**Gap 2. Machine learning models at this stage cannot take full advantage of the rapid progress in computational computing and the high rate of data accumulation.**

Solution: Custom models for individual cases, due to their case-specific nature, leverage the most recently collected data. Moreover, thanks to their lightweight design and targeted optimization based on core characteristics, these models exhibit enhanced training speeds and fully utilize advancements in computing capabilities.

**Gap 3. The current transfer learning approach and lightweight models cannot meet the needs of the industrial and medical fields in terms of the accuracy of models for specific problems, the need for scenario customization, and the need for lightweight devices.**

Solution: Customization for individual cases, coupled with a thorough consideration of specific scene requirements and meticulous optimization based on core characteristics,

results in comprehensive enhancements and validations of model performance in specific scenarios.

## 7.5 Reflection and Limitations

Reflecting on the research methodology and process undertaken in this thesis, several strengths and limitations have emerged, profoundly influencing the interpretation and validity of the findings. The adoption of a scenario-based approach to machine learning model design has been proven to be a significant strength. This method facilitates a targeted and nuanced examination of machine learning models, ensuring high relevance and specificity to individual entities and application scenarios. Particularly, the focus on customization for individual entities and leveraging scenario-specific requirements has demonstrated an innovative departure from traditional one-size-fits-all models, enhancing model interpretability, adaptability, and operational efficiency.

Still, it also underscored the critical balance between model complexity, interpretability, and user acceptance. The pursuit of high accuracy and customization brought to light the trade-offs between model simplicity and the depth of insights required for practical applications. The use of datasets for empirical validation underscored the research design's capability to address real-world problems effectively. By integrating customization and scenario-specific adjustments, the research not only achieved impressive accuracy and performance metrics but also pushed the boundaries of machine learning applications.

However, this research was not without limitations. One of the primary constraints was the reliance on available datasets, which may not fully encapsulate the complexity or variability of real-world scenarios. This limitation potentially impacts the generalizability of the findings beyond the specific contexts examined. Additionally, the computational demands and the need for significant data preprocessing highlight the challenges in deploying these models in resource-constrained environments.

Furthermore, the methodology's intensive focus on customization and scenario specificity may limit the applicability of findings across broader machine learning domains.

While offering deep insights into targeted applications, this approach could overlook emerging challenges in the wider field, such as evolving data privacy concerns and the dynamic nature of data generation in digital ecosystems.

In summary, while the strengths of the research design lie in its innovative approach to machine learning model customization and its application to real-world scenarios, the limitations reflect the inherent challenges of specialized model development. These include potential issues with scalability, generalizability, and the balance between model complexity and practical utility. Future research could explore strategies to mitigate these limitations, possibly through the development of more adaptive models that can dynamically adjust to varied data landscapes without compromising on efficiency or accuracy.

## 7.6 Directions for Future Research

The following are important and desirable directions for continued work that have been summarized during the research process, the completion of which facilitates the further development and generalization of scenario-based machine learning models.

**1. Integration of Temporal Dynamics into Scenario-Based Models.** The inclusion of temporal dynamics within scenario-based machine learning models has been identified as a paramount area for further investigation. It is suggested that future work should concentrate on the development of dynamic models capable of adapting to changes over time. This approach is deemed particularly pertinent for applications within healthcare and industrial monitoring, where the characteristics of entities and scenarios are subject to significant variation.

**2. Advancement in Cross-Scenario Generalization and Transfer Learning.** An exploration into cross-scenario generalization and enhanced transfer learning techniques is recommended. The thesis highlights a substantial opportunity for frameworks that enable the extrapolation of insights and adaptable models across varying yet interconnected scenarios, thereby mitigating the necessity for extensive model retraining. Such research could revolutionize the way models are deployed across different domains, minimizing the

need for training from scratch and fostering a more interconnected, intelligent system of models.

**3. Automation of Model Customization and Optimization.** The automation of the customization and optimization process for machine learning models tailored to specific scenarios represents a significant direction for future research. Investigations should be directed towards employing meta-learning and neural architecture search methodologies, with the aim of facilitating systems that can intuitively adjust models to novel scenarios with minimal external input.

**4. Exploration of Integration with Edge Computing.** The potential integration of scenario-based machine learning models with edge computing technologies emerges as a critical research domain. Such exploration is considered vital for applications necessitating real-time, on-device processing, where decisions are imperative to be made swiftly and autonomously. This research direction holds particular relevance for deployments in autonomous vehicles, smart cities, and the Internet of Things (IoT), where latency and connectivity present significant challenges.

## 7.7 Concluding Remarks

In conclusion, this thesis presents a pioneering framework for the development and application of scenario-based machine learning models, which stands as a notable departure from traditional general-purpose models. This research has systematically demonstrated the advantages of customized machine learning algorithms to specific scenarios, achieving significant improvements in accuracy, efficiency, and adaptability. By addressing the unique requirements of various applications, the thesis underscores the importance of a problem-centric approach, which not only enhances model performance but also aligns with real-world needs.

The findings presented here offer a compelling argument for the continued exploration and refinement of scenario-specific models. This approach promises to bridge existing gaps in machine learning research, particularly in specialized fields such as healthcare and industrial automation, where precision and context-specific adaptations are

crucial. Future research directions, including the integration of temporal dynamics, advancements in transfer learning, automation of model customization, and the potential of edge computing, provide a robust roadmap for further advancing this innovative paradigm.

Ultimately, this work enriches the academic discourse on machine learning, providing both theoretical insights and practical solutions. It advocates for a shift towards more personalized, scenario-aware models, laying a solid foundation for future advancements in the field. This thesis not only contributes to the literature but also offers practical methodologies for developing efficient, accurate, and user-friendly machine learning systems tailored to specific scenarios, thereby opening new avenues for research and application.

The journey through this research has been one of challenging norms and embracing innovation. It is hoped that the contributions of this thesis will inspire continued exploration and refinement of machine learning models, ensuring their relevance and utility in an ever-evolving world. The commitment to pushing the boundaries of what is possible in machine learning, demonstrated by this work, lays a robust foundation for the next generation of researchers and practitioners in the field.

In conclusion, the journey of discovery does not end here but rather marks a new beginning. The insights and methodologies developed in this thesis are stepping stones to further innovations in machine learning. The continued pursuit of knowledge and the application of these findings promise to enrich our understanding and enhance our capabilities in the ever-expanding realm of artificial intelligence.

# APPENDICES

## Algorithm One

In [ ]:

```
# **Loop through each data point in the dataset**
for i = 1 to M do

    # **Define the target patient and update training set**
    x_t = x_i
    Set_train2 = Set_train.remove(x_t)

    # **Initialize Optuna optimizer with N trials**
    for j = 1 to N do

        # **Set hyperparameters (optional fixing)**
        # *Hyperparameters:* bias_coefficient, drop_ratio, epochs
        Assign value to each hyperparameter for this trial

        # **Find samples that satisfy the similarity threshold**
        num_aug = 0
        for k = 1 to M do
            Dist_k = D(x_k, x_t)
            if Dist_k < TH_sim then
                num_aug += 1
            end if
        end for

        # **Form validation set based on closest samples**
        Set_valid = Set_train2.sort(key=Dist_k)[:num_fix]

        # **Oversample minority class if conditions met**
        if num_aug >= 6 and TH_aug >= num_aug / (M - num_aug) then
            # *Oversampling using SMOTE*
            Oversample minority class using x_1 to x_num_aug as base until propo
            Set_train_new = Combine(oversampled_minority, original_majority)
        end if

        # **Return updated training and validation sets**
        return Set_train_new, Set_valid

        # **Normalize data using min-max scaling**
        Set_train_norm, x_t_norm = Normalize(Set_train_new and x_t)

        # **Apply bias to normalized data**
        for k = 1 to M do
            x_k_bias = x_k_norm + e * x_t_norm
        end for

        # **Define Attention Layer according to tf.keras standards**
        class AttLayer:
            def __init__():
                Initialize parent class
                Obtain x_t_norm and dimensionality d

            def build(input_shape):
                Create trainable weight e' with dimension 1, initialized to 0

            def call(inputs):
                x_out = inputs - e' * x_t_norm
                return x_out
        end class
```

```
        model = keras.Sequential([
            AttLayer(),
            Hidden_Layer(),
            Output_Layer()
        ])
        Train model using backpropagation until stopping condition

        # **Return trained model and final loss**
        return Model_trained, final_loss

        # **Optimize hyperparameters based on loss**
        Optuna uses final_loss to plan next trial
        Record best_params from all trials

        j = j + 1
        return best_params
    end for

    # **Predict using the best hyperparameters**
    y_i = Predict(Set_train2, Set_valid, x_t, best_params)

    # **Store the prediction**
    Collect y_i

    i = i + 1
end for

# **Evaluate all predictions against true values**
Compare all y_i with y_true to draw conclusions
```

# Algorithm Two

In [ ]:

```
# **Loop through each data point in the dataset**
for i = 1 to M do

    # **Define the target patient and update training set**
    x_t = x_i
    Set_train2 = Set_train.remove(x_t)

    # **Initialize Optuna optimizer with N trials**
    for j = 1 to N do

        # **Set hyperparameters (optional fixing)**
        # *Hyperparameters:* bias_coefficient, augmentation_threshold, similarit
        Assign value to each hyperparameter for this trial

        # **Find samples that satisfy the similarity threshold**
        num_aug = 0
        for k = 1 to M do
            Dist_k = D(x_k, x_t)
            if Dist_k < TH_sim then
                num_aug += 1
            end if
        end for


        # Determine Set_valid based on the number of augmented samples
        if fixed_number_of_samples_chosen then
            # Set_valid is formed by the first num_fix samples sorted by distanc
            Set_valid = Set_train2.sort(key=Dist_k)[:num_fix]
        else if variable_number_of_samples_chosen then
            if num_aug >= num_min then
                Set_valid = Set_train2.sort(key=Dist_k)[:num_aug]
            else
                Set_valid = Set_train2.sort(key=Dist_k)[:num_min]
            end if
        end if




        # **Oversample minority class if conditions met**
        if num_aug >= 6 and TH_aug >= num_aug / (M - num_aug) then
            # *Oversampling using SMOTE*
            Oversample minority class using x_1 to x_num_aug as base until propc
            Set_train_new = Combine(oversampled_minority, original_majority)
        end if

        if num_aug < 6 then
            no oversampling is performed, and the target patient is marked as a
        end if

        if TH_aug < num_aug / (M - num_aug) then
            no oversampling is performed.
        end if




        # **Return updated training and validation sets**
```

```
        return Set_train_new, Set_valid

        # **Normalize data using min-max scaling**
        Set_train_norm, x_t_norm = Normalize(Set_train_new and x_t)

        # **Apply bias to normalized data**
        for k = 1 to M do
            x_k_bias = x_k_norm + e * x_t_norm
        end for

        # **Define Attention Layer according to tf.keras standards**
        class AttLayer:
            def __init__():
                Initialize parent class
                Obtain x_t_norm and dimensionality d

            def build(input_shape):
                Create trainable weight e' with dimension 1, initialized to 0

            def call(inputs):
                x_out = inputs - e' * x_t_norm
                return x_out
        end class


        model = keras.Sequential([
            AttLayer(),
            Hidden_Layer(),
            Output_Layer()
        ])
        Train model using backpropagation until stopping condition

        # **Return trained model and final loss**
        return Model_trained, final_loss

        # **Optimize hyperparameters based on loss**
        Optuna uses final_loss to plan next trial
        Record best_params from all trials

        j = j + 1
        return best_params
    end for

    # **Predict using the best hyperparameters**
    y_i = Predict(Set_train2, Set_valid, x_t, best_params)

    # **Store the prediction**
    Collect y_i

    i = i + 1
end for

# **Evaluate all predictions against true values**
Compare all y_i with y_true to draw conclusions
```

# Algorithm Three

In [ ]:

```
# **Customized Obstacle Detection System with Detailed Problem Setup**

# **Imports and Constants**
import ExternalMemory
import Sensors  # e.g., Camera, LiDAR, GPS/IMU
import NeuralNetworks  # For F_Detect and F_diff

# **Global Variables**
global_map = initialize_global_map()  # m^g ∈ R^(h×w×L×C×E)

# **Functions and Classes**

# **Class: GlobalMap**
class GlobalMap:
    def __init__(self, h, w, L, C, E):
        self.map = initialize_map(h, w, L, C, E)  # m^g

    def query_standard_image(self, P_ego):
        # Extract I^s based on P_ego ∈ R^(L×C×E)
        I_s = self.map.get_observation(P_ego)
        return I_s

    def update_map(self, P_ego, I_t_s):
        # Replace I_(t-1)^s with I_t^s in the global map
        self.map.set_observation(P_ego, I_t_s)

# **Function: F_Detect**
def F_Detect(I):
    # Standard object detection model (e.g., YOLO)
    BBox, LIn, Con = NeuralNetworks.F_Detect(I)
    return BBox, LIn, Con

# **Function: F_diff**
def F_diff(I, I_s):
    # Difference function to generate refined road image
    I_refine = I - I_s  # Assuming image subtraction
    return I_refine

# **Function: LSTM_Update**
def LSTM_Update(I_update, I_prev_s, C_prev,
                W_u, W_f, W_o, W_m,
                b_u, b_f, b_o, b_m):
    # Concatenate I_prev_s and I_update
    concat_input = concat(I_prev_s, I_update)

    # Compute gates
    Γ_u = sigmoid(dot(W_u, concat_input) + b_u)  # (60)
    Γ_f = sigmoid(dot(W_f, concat_input) + b_f)  # (61)
    Γ_o = sigmoid(dot(W_o, concat_input) + b_o)  # (62)

    # Compute candidate cell state
    C_t_l_tilde = tanh(dot(W_m, concat_input) + b_m)  # (63)

    # Update cell state
    C_t_l = Γ_u ⊙ C_t_l_tilde + Γ_f ⊙ C_prev  # (64)

    # Compute new standard image
    I_t_s = Γ_o ⊙ tanh(C_t_l)  # (65)
```

```
    return I_t_s, C_t_l

# **Function: Result_Fusion**
def Result_Fusion(BBox, LIn, Con,
                  BBox_refine, LIn_refine, Con_refine, ratio):
    # Layer detections with predetermined ratio
    fused_BBox = layer(BBox, BBox_refine, ratio)
    fused_LIn = layer(LIn, LIn_refine, ratio)
    fused_Con = layer(Con, Con_refine, ratio)
    return fused_BBox, fused_LIn, fused_Con

# **Main Processing Function**
def main_process(I, P_ego, global_map, LSTM_params, C_prev):
    # **Step 1: Standard Detection**
    BBox, LIn, Con = F_Detect(I)  # (56)

    # **Step 2: Retrieve Standard Image from Global Map**
    I_s = global_map.query_standard_image(P_ego)

    # **Step 3: Compute Refined Road Image**
    I_refine = F_diff(I, I_s)  # (57)

    # **Step 4: Fast Detection on Refined Image**
    BBox_refine, LIn_refine, Con_refine = F_Detect(I_refine)  # (58)

    # **Step 5: Compute Background Information for Map Update**
    I_update = I - I_refine  # Background information

    # **Step 6: LSTM-Based Map Update**
    I_t_s, C_t_l = LSTM_Update(
        I_update,
        I_s,
        C_prev,
        LSTM_params.W_u, LSTM_params.W_f,
        LSTM_params.W_o, LSTM_params.W_m,
        LSTM_params.b_u, LSTM_params.b_f,
        LSTM_params.b_o, LSTM_params.b_m
    )

    # **Step 7: Update Global Map**
    global_map.update_map(P_ego, I_t_s)

    # **Step 8: Fuse Detection Results**
    fused_BBox, fused_LIn, fused_Con = Result_Fusion(
        BBox, LIn, Con,
        BBox_refine, LIn_refine, Con_refine,
        ratio=0.5  # Example ratio
    )

    return fused_BBox, fused_LIn, fused_Con, I_t_s, C_t_l

# **Helper Functions**

def initialize_global_map():
    # Initialize global map m^g ∈ R^(h×w×L×C×E)
    h, w, L, C, E = get_map_dimensions()
    return GlobalMap(h, w, L, C, E)
```

```
def layer(data1, data2, ratio):
    # Layer two datasets with a given ratio
    return ratio * data1 + (1 - ratio) * data2

# **Initialization**
def initialize_system():
    # Initialize global map and LSTM parameters
    global_map = initialize_global_map()
    LSTM_params = load_LSTM_parameters()
    C_prev = initialize_cell_state()
    return global_map, LSTM_params, C_prev

# **Execution**
def execute():
    # Initialize system components
    global_map, LSTM_params, C_prev = initialize_system()

    while True:
        # Acquire sensor data
        I, P_ego = Sensors.get_camera_data()

        # Process the frame
        fused_BBox, fused_LIn, fused_Con, I_t_s, C_t_l = main_process(
            I,
            P_ego,
            global_map,
            LSTM_params,
            C_prev
        )

        # Update cell state for next iteration
        C_prev = C_t_l

        # Output the final detection results
        display_results(fused_BBox, fused_LIn, fused_Con)

# **Start Execution**
execute()
```

# REFERENCES


A, C., M, B., A, G., & Petr, S. S. Development of Intelligent Obstacle Detection System on Railway Tracks for Yard Locomotives Using CNN. *EDCC Workshops*. doi:10.1007/978-3-030-58462-7_3

A, C., & M, G. S. Fairer and more accurate, but for whom? *arXiv.org*.

A, D. A., K, H., D, M., Ben, A., B, A., Alex, B., . . . D, S. Underspecification Presents Challenges for Credibility in Modern Machi ne Learning. *Journal of machine learning research*.

A, F. C., K, L., & Christopher, D. S. Accuracy-Efficiency Trade-Offs and Accountability in Distributed ML Sy stems. *Conference on Equity and Access in Algorithms, Mechanisms, and Optimiz ation*. doi:10.1145/3465416.3483289

A, F. C., K, L., & Christopher, D. S. Holding Real-Time Distributed ML Systems to Account.

A, G., Mark, G. G., Kathryn, K. R., A, N., Virginia, P., Shamanth, R. K., . . . Manpreet, K. S. Applying Machine Learning to Increase Efficiency and Accuracy of Meta- Analytic Review. *bioRxiv*. doi:10.1101/2020.10.06.314245

A, K. Analysis of hidden feedback loops in continuous machine learning syste ms. *International Conference on Software Quality. Process Automation in So ftware Development*. doi:10.1007/978-3-030-65854-0_5

Á, M.-M., M, P., J, M.-M., M, C.-T., J, A., Anna, M., . . . Gustau, C.-V. Machine Learning Methods for Spatial and Temporal Parameter Estimation. doi:10.1007/978-3-030-38617-7_2

A, O., Scott, C., & T, K. Hepatitis C Diagnostics Technology Landscape.

A, P., & J, A. B. High dimensionality: The latest challenge to data analysis.

A, Q., Junaid, Q., M, B., & Ala, I. A.-F. Secure and Robust Machine Learning for Healthcare: A Survey. *IEEE Reviews in Biomedical Engineering*. doi:10.1109/RBME.2020.3013489

A, R., Tri-Long, N., P, D., A, F., Naja, H., & Claus, T. E. Machine learning models aimed at identifying risk factors for reducing morbidity and mortality still need to consider confounding related to calendar time variations. *medRxiv*. doi:10.1101/2022.05.24.22275482

A, S. Adaptive Machine Learning for Robust Diagnostics and Control of Time-V arying Particle Accelerator Components and Beams. *Inf.* doi:10.20944/PREPRINTS202103.0301.V1

A, S., C, V., Z, Z., D, R., S, M., D, Z., . . . C, B. Decision Support by Interpretable Machine Learning in Acoustic Emissio n Based Cutting Tool Wear Prediction. *IEEE International Conference on Industrial Engineering and Engineerin g Management*. doi:10.1109/IEEM50564.2021.9673044

A'fifah, A. i., Ritahani, A., & Ahmad, A. Comparative Performance of Deep Learning and Machine Learning Algorith ms on Imbalanced Handwritten Data. *International Journal of Advanced Computer Science and Applications, 9*(2). doi:10.14569/ijacsa.2018.090236

Aasheesh, S., H, P., Jacob, M., Arun, P. S., Laxmi, N., & Amit, S. Enhancing Security and Privacy in Cloud – Based Healthcare Data Throug h Machine Learning. *2023 International Conference on Artificial Intelligence for Innovatio ns in Healthcare Industries (ICAIIHI)*. doi:10.1109/ICAIIHI57871.2023.10489735

Abadi, M., Barham, P., Chen, J., Chen, Z., Davis, A., Dean, J., . . . Isard, M. (2016). *{TensorFlow}: A System for {Large-Scale} Machine Learning.* Paper presented at the 12th USENIX symposium on operating systems design and implementation (OSDI 16).

Abd Aziz, A. Z. Effects of Visible and Near Infrared Polarized Lights on Spoofing Face Detection. *Journal of Computer Science, 15*(2), 288-301. doi:10.3844/jcssp.2019.288.301

Abhijeet, K., & Avinash, S. DEEP-LEARNING FEATURES, GRAPHS AND SCENE UNDERSTANDING.

Abokadr, S., Azman, A., Hamdan, H., & Amelina, N. (2023/10/10/). *Handling Imbalanced Data for Improved Classification Performance: Meth ods and Challenges*.

Adam, C., A, N., & Honglak, L. An Analysis of Single-Layer Networks in Unsupervised Feature Learning. *International Conference on Artificial Intelligence and Statistics*.

Adam, L., Tom'avs, K. y., E, G., Tayfun, T., Eren, S., Devang, A., . . . Angeliki, L. StreamingQA: A Benchmark for Adaptation to New Knowledge over Time in Question Answering Models. *International Conference on Machine Learning*.

Adu-Gyamfi, Y. O., Asare, S. K., Sharma, A., & Titus, T. Automated Vehicle Recognition with Deep Convolutional Neural Networks. *Transportation Research Record: Journal of the Transportation Research Board, 2645*(1), 113-122. doi:10.3141/2645-13

Aduri, U. K. R., Kuchipudi, P. K., & Prakash, M. (2023). *Agro Prognostics Based on Characteristics of the Agricultural Environm ent Using Machine Learning*.

Agarwal, S. (2020). *Trade-offs between fairness, interpretability, and privacy in machine learning.* University of Waterloo,

Agarwal, S. (2021). *Trade-offs between fairness and privacy in machine learning.* Paper presented at the IJCAI 2021 Workshop on AI for Social Good.

Agrawal, T. (2021). *Hyperparameter optimization in machine learning: make your machine learning and deep learning models more efficient*: Springer.

Ahamed, S. I., & Ravi, V. Privacy-Preserving Chaotic Extreme Learning Machine with Fully Homomor phic Encryption. *arXiv.org*. doi:10.48550/ARXIV.2208.02587

Ahsan, M. M., & Siddique, Z. (2022). Machine learning-based heart disease diagnosis: A systematic literature review. *Artificial Intelligence in Medicine*, 102289.

AI-Driven Automated Feature Engineering to Enhance Performance of Pred ictive Models in Data Science. *International Journal of Control and Automation*. doi:10.52783/ijca.v13i4.38349

Aickelin, U., Khorshidi, H. A., Qu, R., & Charkhgard, H. Guest Editorial Special Issue on Multiobjective Evolutionary Optimizat ion in Machine Learning. *IEEE Transactions on Evolutionary Computation, 27*(4), 746-748. doi:10.1109/tevc.2023.3292528

Akella, A., & Akella, S. Applying Machine Learning to Evaluate for Fibrosis in Chronic Hepatiti s C. *medRxiv*. doi:10.1101/2020.11.02.20224840

Akhter, J., Fährmann, P. D., Sonntag, K., & Peitz, S. Common pitfalls to avoid while using multiobjective optimization in ma chine learning. *arXiv.org*. doi:10.48550/ARXIV.2405.01480

Akhuseyinoglu, K., & Brusilovsky, P. Exploring Behavioral Patterns for Data-Driven Modeling of Learners' In dividual Differences. *Frontiers in Artificial Intelligence, 5*. doi:10.3389/frai.2022.807320

Akiba, T., Sano, S., Yanase, T., Ohta, T., & Koyama, M. (2019a). *Optuna: A next-generation hyperparameter optimization framework.* Paper presented at the Proceedings

of the 25th ACM SIGKDD international conference on knowledge discovery & data mining.

Akiba, T., Sano, S., Yanase, T., Ohta, T., & Koyama, M. (2019b). *Optuna: A next-generation hyperparameter optimization framework.* Paper presented at the Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery \& data mining.

Al Daoud, E. (2019). Comparison between XGBoost, LightGBM and CatBoost using a home credit dataset. *International Journal of Computer and Information Engineering, 13*(1), 6-10.

Al Olaby, R. R., & Azzazy, H. M. (2011). Hepatitis C virus RNA assays: current and emerging technologies and their clinical applications. *Expert review of molecular diagnostics, 11*(1), 53-64.

Alabadla, M., Sidi, F., Ishak, I., Ibrahim, H., Affendey, L. S., Ani, Z. C., . . . Muda, A. S. (2022). Systematic review of using machine learning in imputing missing values. *IEEE Access, 10*, 44483-44502.

Alamri, F., & Pugeault, N. Improving Object Detection Performance Using Scene Contextual Constrai nts. *IEEE Transactions on Cognitive and Developmental Systems, 14*(4), 1320-1330. doi:10.1109/tcds.2020.3008213

Alan, W., A, M., James, W., Johanna, M., & V, B. Effective resource management using machine learning in medicine: an a pplied example. *BMJ Simulation and Tecnnology Enhanced Learning*. doi:10.1136/bmjstel-2017-000289

Alberto, M., M, H., Faiq, K., George, P., C, K., T, T., & M, S. Deep Learning for Edge Computing: Current Trends, Cross-Layer Optimiza tions, and Open Research Challenges. *IEEE Computer Society Annual Symposium on VLSI*. doi:10.1109/ISVLSI.2019.00105

Alessia, L., D, D. A., & M, M. Comparison of Machine Learning Models for Predictive Maintenance Appli cations. *SYSINT*. doi:10.1007/978-3-031-16281-7_62

Alexander, H., Dorota, R., Elisabeth, P., & N, J. Using Smartphone Sensor Paradata and Personalized Machine Learning Mod els to Infer Participants' Well-being: Ecological Momentary Assessment. *Journal of Medical Internet Research*. doi:10.2196/34015

Alexandra, Z., Dongyu, L., R, V., & K, V. Understanding the Usability Challenges of Machine Learning In High-Sta kes Decision Making. *arXiv.org*.

Alexandra, Z., Ignacio, A., Dongyu, L., Laure, B.-É., & K, V. The Need for Interpretable Features. *SIGKDD Explorations*. doi:10.1145/3544903.3544905

Almlund, M., Duckworth, A. L., Heckman, J., & Kautz, T. *Personality Psychology and Economics*. Retrieved from http://dx.doi.org/10.3386/W16822

Alom, M. Z., Taha, T. M., Yakopcic, C., Westberg, S., Sidike, P., Nasrin, M. S., . . . Asari, V. K. (2018). The history began from alexnet: A comprehensive survey on deep learning approaches. *arXiv preprint arXiv:1803.01164*.

Alqaissi, E. Y., Alotaibi, F. S., & Ramzan, M. S. Modern Machine-Learning Predictive Models for Diagnosing Infectious Di seases. *Computational and Mathematical Methods in Medicine, 2022*, 1-13. doi:10.1155/2022/6902321

Alter, M. J. (1997). Epidemiology of hepatitis C. *Hepatology, 26*, 62S-65S.

Alwosheel, A., van Cranenburgh, S., & Chorus, C. G. (2018). Is your dataset big enough? Sample size requirements when using artificial neural networks for discrete choice analysis. *Journal of choice modelling, 28*, 167-182.

Amelia, T. S., Hasibuan, M. N. S., & Pane, R. Comparative analysis of resampling techniques on Machine Learning algo rithm. *Sinkron, 7*(2), 628-634.

doi:10.33395/sinkron.v7i2.11427

Amerise, I. L., & Tarsitano, A. A New Method to Detect Outliers in High-frequency Time Series. *International Journal of Statistics and Probability, 8*(1), 16. doi:10.5539/ijsp.v8n1p16

Amin, M. S., Chiam, Y. K., & Varathan, K. D. (2019). Identification of significant features and data mining techniques in predicting heart disease. *Telematics and Informatics, 36*, 82-93.

Amirali, S.-A., & Craig, B. Preference-oriented Social Networks: Group Recommendation and Inferenc e. *ACM Conference on Recommender Systems*. doi:10.1145/2792838.2800190

Anant, A., & Prasad, R. The New Social Necessity – Data Privacy. *Journal of Mobile Multimedia*. doi:10.13052/jmm1550-4646.171314

Andras Janosi, W. S., Matthias Pfisterer, Robert Detrano. (1988). *Heart Disease Data Set*. Retrieved from: https://archive.ics.uci.edu/ml/datasets/Heart+Disease

Andrea, C., Lorenzo, F., A, C., & F, C. Everything is varied: The surprising impact of instantial variation on ML reliability. *Applied Soft Computing*. doi:10.1016/j.asoc.2023.110644

Andrei, P., Raoul-Gabriel, U., & Neil, D. L. Challenges in Deploying Machine Learning: A Survey of Case Studies. *ACM Computing Surveys*. doi:10.1145/3533378

Angati, K. Feature Contribution to an In-Depth Understanding of the Machine Learn ing Model Interpretation. *Przeglad Elektrotechniczny*. doi:10.15199/48.2024.02.29

Angela, L., Doris, X., D, L., & Aditya, G. P. Demystifying a Dark Art: Understanding Real-World Machine Learning Mod el Development. *arXiv.org*.

Angeliki, L., A, K., E, G., Devang, A., Adam, L., Tayfun, T., . . . Phil, B. Pitfalls of Static Language Modelling. *arXiv.org*.

Anmar, A. A.-J., Sufyan, T. F. A.-J., & Belal, A.-K. Secure Data Computation Using Deep Learning and Homomorphic Encryption : A Survey. *Int. J. Online Biomed. Eng.* doi:10.3991/ijoe.v19i11.40267

Anupama, K., Himanshu, G., & Digvijay, S. L. Impact of feature selection and engineering in the classification of h andwritten text. *International Conference on Computing for Sustainable Global Developme nt*.

Apostolos, G., Víctor, V., G, I., & D, L. Measurement-driven Analysis of an Edge-Assisted Object Recognition Sys tem. *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*. doi:10.1109/ICC40277.2020.9149069

Arantes, R. B., Vogiatzis, G., & Faria, D. R. Learning an augmentation strategy for sparse datasets. *Image and Vision Computing, 117*, 104338. doi:10.1016/j.imavis.2021.104338

Arca-Lafuente, S., Martínez-Román, P., Mate-Cano, I., Madrid, R., & Briz, V. Nanotechnology: A reality for diagnosis of HCV infectious disease. *Journal of Infection, 80*(1), 8-15. doi:10.1016/j.jinf.2019.09.010

Archer, M. S. (1995). *Realist social theory: The morphogenetic approach*: Cambridge university press.

Arik, S. Ö., & Pfister, T. (2021). *Tabnet: Attentive interpretable tabular learning.* Paper presented at the Proceedings of the AAAI Conference on Artificial Intelligence.

Arivoli, A., & Paul, S. B. Predicting Human Activity and Behavior Patterns from Cell Phone Data U sing Machine Learning. *International Research Journal of Multidisciplinary Scope, 05*(01), 113-123. doi:10.47857/irjms.2024.v05i01.0165

Arnab, P., & Suresh, V. Why does Deep Learning work? - A perspective from Group Theory. *arXiv.org*.

Arnaud, G. S., Marina, C., Oana, S., Renaud, S., & Cédric, G.-P. Combining homomorphic encryption and differential privacy in federated learning. *Conference on Privacy, Security and Trust*. doi:10.1109/PST58708.2023.10320195

Arvind, N., Joanna, H., & E, F. A Precautionary Approach to Big Data Privacy. doi:10.1007/978-94-017-7376-8_13

Aryal, S., Do, T., Heyojoo, B., Chataut, S., Gurung, B. D. S., Gadhamshetty, V., & Gnimpieba, E. Leveraging Multi-AI Agents for Cross-Domain Knowledge Discovery. *arXiv.org*. doi:10.48550/ARXIV.2404.08511

Asuero, A. G., Sayago, A., & González, A. (2006). The correlation coefficient: An overview. *Critical reviews in analytical chemistry, 36*(1), 41-59.

Atla, A., Tada, R., Sheng, V., & Singireddy, N. (2011). Sensitivity of different machine learning algorithms to noise. *Journal of Computing Sciences in Colleges, 26*(5), 96-103.

Attila, F., Gábor, K., & R, L. Parallel and Distributed Training of Deep Neural Networks: A brief ove rview. *International Conference on Intelligent Engineering Systems*. doi:10.1109/INES49302.2020.9147123

Aycan, A., Tizian, M., Maike, G., S, T., & L, K. At What Price? Exploring the Potential and Challenges of Differentiall y Private Machine Learning for Healthcare. *Hawaii International Conference on System Sciences*. doi:10.24251/hicss.2023.403

Ayer, A. J. (1959). *Logical positivism* (Vol. 2): Simon and Schuster.

Aziz, R., Banerjee, S., Bouzefrane, S., & Le Vinh, T. Exploring Homomorphic Encryption and Differential Privacy Techniques t owards Secure Federated Learning Paradigm. *Future Internet, 15*(9), 310. doi:10.3390/fi15090310

B, C., & J, V. Adaptation Strategies for Automated Machine Learning on Evolving Data. *IEEE transactions on pattern analysis and machine intelligence*. doi:10.1109/TPAMI.2021.3062900

B, G., Charles, J., Mélanie, B., & S, W. Algorithmic encoding of protected characteristics and its implications on performance disparities.

Bach, F. R., & Jordan, M. I. (2005). *Predictive low-rank decomposition for kernel methods.* Paper presented at the Proceedings of the 22nd international conference on Machine learning.

Badirli, S., Liu, X., Xing, Z., Bhowmik, A., Doan, K., & Keerthi, S. S. (2020). Gradient boosting neural networks: Grownet. *arXiv preprint arXiv:2002.07971*.

Bai, J., Lu, F., & Zhang, K. (2019). Onnx: Open neural network exchange. *GitHub repository*.

Bakshi, A., & Gupta, S. Face Anti-Spoofing System using Motion and Similarity Feature Eliminat ion under Spoof Attacks. *The International Arab Journal of Information Technology, 19*(5). doi:10.34028/iajit/19/5/6

Bałdyga, M., Barański, K., Belter, J., Kalinowski, M., & Weichbroth, P. Anomaly Detection in Railway Sensor Data Environments: State-of-the-Ar t Methods and Empirical Performance Evaluation. *Sensors, 24*(8), 2633. doi:10.3390/s24082633

Baltrusaitis, T., Ahuja, C., & Morency, L.-P. Multimodal Machine Learning: A Survey and Taxonomy. *IEEE transactions on pattern analysis and machine intelligence, 41*(2), 423-443. doi:10.1109/tpami.2018.2798607

Bansal, K., & Jain, V. (2020/3//). *Performance Analysis of Collaborative Filtering based Recommendation S ystem on Similarity Threshold*.

Barbosa, N. M., Park, J. S., Yao, Y., & Wang, Y. “What if?” Predicting Individual Users’ Smart Home Privacy Pref erences and Their Changes. *Proceedings on Privacy Enhancing Technologies, 2019*(4), 211-231. doi:10.2478/popets-2019-0066

Barenholtz, E., Fitzgerald, N. D., & Hahn, W. E. Machine-learning approaches to substance-abuse research: emerging tren ds and their implications. *Current Opinion in Psychiatry, 33*(4), 334-342. doi:10.1097/yco.0000000000000611

Barham, P., & Isard, M. (2019/5/13/). *Machine Learning Systems are Stuck in a Rut*.

Barlow, H. B. (1989). Unsupervised learning. *Neural computation, 1*(3), 295-311.

Barron, J. T. (2019). *A general and adaptive robust loss function.* Paper presented at the Proceedings of the IEEE/CVF conference on computer vision and pattern recognition.

Barua, A., Ahmed, M. U., & Begum, S. A Systematic Literature Review on Multimodal Machine Learning: Applica tions, Challenges, Gaps and Future Directions. *IEEE Access, 11*, 14804-14831. doi:10.1109/access.2023.3243854

Bassily, R., Smith, A., & Thakurta, A. (2014). *Private empirical risk minimization: Efficient algorithms and tight error bounds.* Paper presented at the 2014 IEEE 55th annual symposium on foundations of computer science.

Beaulieu-Jones, B. K., Yuan, W., Brat, G. A., Beam, A. L., Weber, G., Ruffin, M., & Kohane, I. S. Machine learning for patient risk stratification: standing on, or look ing over, the shoulders of clinicians? *npj Digital Medicine, 4*(1). doi:10.1038/s41746-021-00426-3

Behrens, J. T. (1997). Principles and procedures of exploratory data analysis. *Psychological methods, 2*(2), 131.

Belkin, M., Hsu, D., Ma, S., & Mandal, S. Reconciling modern machine-learning practice and the classical bias–va riance trade-off. *Proceedings of the National Academy of Sciences, 116*(32), 15849-15854. doi:10.1073/pnas.1903070116

Bell, A., Solano-Kamaiko, I., Nov, O., & Stoyanovich, J. (2022/6/20/). *It’s Just Not That Simple: An Empirical Study of the Accuracy-Explaina bility Trade-off in Machine Learning for Public Policy*.

Bellamy, R. K. E., Dey, K., Hind, M., Hoffman, S. C., Houde, S., Kannan, K., . . . Zhang, Y. Think Your Artificial Intelligence Software Is Fair? Think Again. *IEEE Software, 36*(4), 76-80. doi:10.1109/ms.2019.2908514

Bergman, M. E., Donovan, M. A., Drasgow, F., Overton, R. C., & Henning, J. B. Test of Motowidlo et al.'s (1997) Theory of Individual Differences in Task and Contextual Performance. *Human Performance, 21*(3), 227-253. doi:10.1080/08959280802137606

Berrar, D., Lopes, P., & Dubitzky, W. Incorporating domain knowledge in machine learning for soccer outcome prediction. *Machine learning, 108*(1), 97-126. doi:10.1007/s10994-018-5747-8

Bertolini, M., Mezzogori, D., Neroni, M., & Zammori, F. (2021). Machine Learning for industrial applications: A comprehensive literature review. *Expert Systems with Applications, 175*, 114820.

Bertrand, L. S. Modèles d'Apprentissage Machine pour la Compréhension de Scènes. (Mach ine Learning Models for Scene Understanding).

Bhat, G., Danelljan, M., Van Gool, L., & Timofte, R. (2020). Know Your Surroundings: Exploiting Scene Information for Object Tracki ng. In *Lecture Notes in Computer Science* (pp. 205-221): Springer International Publishing.

Bhatia, A., Varakantham, P., & Kumar, A. (2019). *Resource constrained deep reinforcement learning.* Paper presented at the Proceedings of the International Conference on Automated Planning and Scheduling.

Bhatt, U., Ravikumar, P., & Moura, J. e. M. F. Building Human-Machine Trust via Interpretability. *Proceedings of the AAAI Conference on Artificial Intelligence, 33*(01), 9919-9920. doi:10.1609/aaai.v33i01.33019919

Bhattacharya, A., Stumpf, S., & Verbert, K. (2024/6/27/). *An Explanatory Model Steering System for Collaboration between Domain Experts and AI*.

Bhattacharya, S. Some Salient Aspects of Machine Learning Research: A Bibliometric Anal ysis. *Journal of Scientometric Research, 8*(2s), s85-s92. doi:10.5530/jscires.8.2.26

Bi, X., Gao, H., Chen, H., Wang, P., & Ma, C. (2022/8//). *Evaluating the Robustness of Object Detection in Autonomous Driving Sy stem*.

Bichen, W., F, I., Peter, H. J., & K, K. SqueezeDet: Unified, Small, Low Power Fully Convolutional Neural Netwo rks for Real-Time Object Detection for Autonomous Driving. *2017 IEEE Conference on Computer Vision and Pattern Recognition Worksh ops (CVPRW)*. doi:10.1109/CVPRW.2017.60

Bilwaj, G. P. D., Kirstin, C., Luke, M., Eb, L. M., & Ai, T. AI Ethics Journal.

Binjubeir, M., Ahmed, A. A., Ismail, M. A. B., Sadiq, A. S., & Khan, M. K. (2019). Comprehensive survey on big data privacy protection. *IEEE Access, 8*, 20067-20079.

Bishop, C. M. (2013). Model-based machine learning. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 371*(1984), 20120222.

Björneld, O., Löwe, W., & Carlsson, M. Case Study - Feature Engineering Inspired by Domain Experts on Real Wo rld Medical Data. *SSRN Electronic Journal*. doi:10.2139/ssrn.4169773

Blanchard, M. (2024). *Fundamental Limits of Learning for Generalizability, Data Resilience, and Resource Efficiency.* Massachusetts Institute of Technology,

Blaž, Š., S, D., N, L., & Matej, P. Feature Importance Estimation with Self-Attention Networks. *European Conference on Artificial Intelligence*. doi:10.3233/FAIA200256

Bocca, F. F., & Rodrigues, L. H. A. The effect of tuning, feature engineering, and feature selection in da ta mining applied to rainfed sugarcane yield modelling. *Computers and electronics in agriculture, 128*, 67-76. doi:10.1016/j.compag.2016.08.015

Boenisch, F., Battis, V., Buchmann, N., & Poikela, M. (2021/9/5/). *"I Never Thought About Securing My Machine Learning Systems": A Study of Security and Privacy Awareness of Machine Learning Practitioners*.

Bojar, O., Buck, C., Federmann, C., Haddow, B., Koehn, P., Leveling, J., . . . Saint-Amand, H. (2014). *Findings of the 2014 workshop on statistical machine translation.* Paper presented at the Proceedings of the ninth workshop on statistical machine translation.

Borghesi, A., Baldo, F., Lombardi, M., & Milano, M. (2020). Injective Domain Knowledge in Neural Networks for Transprecision Compu ting. In *Lecture Notes in Computer Science* (pp. 587-600): Springer International Publishing.

Borisov, V., Leemann, T., Seßler, K., Haug, J., Pawelczyk, M., & Kasneci, G. (2022). Deep neural networks and tabular data: A survey. *IEEE Transactions on Neural Networks and Learning Systems*.

Bosnic, Z., & Kononenko, I. (2011). Reliability Estimates for Regression Predictions. In *Integrations of Data Warehousing, Data Mining and Database Technologie s* (pp. 320-338): IGI Global.

Bosnić, Z., & Kononenko, I. An overview of advances in reliability estimation of individual predic tions in machine learning. *Intelligent Data Analysis, 13*(2), 385-401. doi:10.3233/ida-2009-0371

Bosnić, Z., & Kononenko, I. (2008). Empirical Analysis of Reliability Estimates for Individual Regression Predictions. In *Lecture Notes in Computer Science* (pp. 379-388): Springer Berlin Heidelberg.

Bottou, L., & Bousquet, O. (2007). The tradeoffs of large scale learning. *Advances in Neural Information Processing Systems, 20*.

Boukortt, N., Patanè, S., & Crupi, G. (2020). 3D investigation of 8-nm tapered n-FinFET model. *Silicon, 12*(7), 1585-1591.

Bousquet, O., & Elisseeff, A. (2002). Stability and generalization. *The Journal of Machine Learning Research, 2*, 499-526.

Bradski, G. (2000). The opencv library. *Dr. Dobb's Journal: Software Tools for the Professional Programmer, 25*(11), 120-123.

Brazdil, P., van Rijn, J. N., Soares, C., & Vanschoren, J. (2022). Dataset Characteristics (Metafeatures). In *Cognitive Technologies* (pp. 53-75): Springer International Publishing.

Briand, L., Bianculli, D., Nejati, S., Pastore, F., & Sabetzadeh, M. (2017). The case for context-driven software engineering research: generalizability is overrated. *IEEE Software, 34*(5), 72-75.

Brodley, C. E., Rebbapragada, U., Small, K., & Wallace, B. (2012). Challenges and opportunities in applied machine learning. *Ai Magazine, 33*(1), 11-24.

Brown, T., Mann, B., Ryder, N., Subbiah, M., Kaplan, J. D., Dhariwal, P., . . . Askell, A. (2020). Language models are few-shot learners. *Advances in neural information processing systems, 33*, 1877-1901.

Brucker, M., Cramariuc, A., Von Einem, C., Siegwart, R., & Cadena, C. (2023/10/1/). *Local and Global Information in Obstacle Detection on Railway Tracks*.

Bryman, A. (2016). *Social research methods*: Oxford university press.

Buda, M., Maki, A., & Mazurowski, M. A. A systematic study of the class imbalance problem in convolutional neu ral networks. *Neural networks, 106*, 249-259. doi:10.1016/j.neunet.2018.07.011

Budholiya, K., Shrivastava, S. K., & Sharma, V. (2022). An optimized XGBoost based diagnostic system for effective prediction of heart disease. *Journal of King Saud University-Computer and Information Sciences, 34*(7), 4514-4523.

Budzan, S., & Kasprzyk, J. (2016). Fusion of 3D laser scanner and depth images for obstacle recognition in mobile applications. *Optics and Lasers in Engineering, 77*, 230-240.

Burstow, N. J., Mohamed, Z., Gomaa, A. I., Sonderup, M. W., Cook, N. A., Waked, I., . . . Taylor-Robinson, S. D. (2017). Hepatitis C treatment: where are we now? *International journal of general medicine*, 39-52.

Byron, C. W., Kevin, S., C, B., & T, T. Class Imbalance, Redux. *2011 IEEE 11th International Conference on Data Mining*. doi:10.1109/ICDM.2011.33

C, R. Please Stop Explaining Black Box Models for High Stakes Decisions. *arXiv.org*.

Cai, C. J., Reif, E., Hegde, N., Hipp, J., Kim, B., Smilkov, D., . . . Stumpe, M. C. (2019). *Human-centered tools for coping with imperfect algorithms during medical decision-making.* Paper presented at the Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems.

Cai, Z., He, X., Sun, J., & Vasconcelos, N. (2017). *Deep learning with low precision by half-wave gaussian quantization.* Paper presented at the Proceedings of the IEEE conference on computer vision and pattern recognition.

Campos, J., & De Rus, G. (2009). Some stylized facts about high-speed rail: A review of HSR experiences around the world. *Transport policy, 16*(1), 19-28.

Cannarsa, M. (2021). Ethics Guidelines for Trustworthy AI. In *The Cambridge Handbook of Lawyering in the Digital Age* (pp. 283-297): Cambridge University Press.

Cao, J., Li, Y., & Du, S. Robust Artificial Intelligence-Aided Multimodal Rail-Obstacle Detectio n Method by Rail Track Topology Reconstruction. *Applied Sciences, 14*(7), 2795. doi:10.3390/app14072795

Cao, V.-H., Chu, K., Le-Khac, N.-A., Kechadi, M. T., Laefer, D., & Truong-Hong, L. (2015). *Toward a new approach for massive LiDAR data processing.* Paper presented at the 2015 2nd IEEE International Conference on Spatial Data Mining and Geographical Knowledge Services (ICSDM).

Cao, Z., Sun, D., Wang, S., Zhang, Y., Feng, Y., & Jiang, S. (2022). R-TDBF: An Environmental Adaptive Method for RFID Redundant Data Filte ring. In *Lecture Notes in Computer Science* (pp. 582-594): Springer Nature Switzerland.

Carbonell, J. G., Michalski, R. S., & Mitchell, T. M. (1983). An overview of machine learning. *Machine learning*, 3-23.

Carion, N., Massa, F., Synnaeve, G., Usunier, N., Kirillov, A., & Zagoruyko, S. (2020). *End-to-end object detection with transformers.* Paper presented at the European Conference on Computer Vision.

Caroline, M. M. The Relationship Between Job Characteristics and Employee Performance: A Review.

Carpenter, C. Psychological Factors Coupled With Machine Learning Improve Rig Traini ng. *Journal of Petroleum Technology, 74*(08), 75-77. doi:10.2118/0822-0075-jpt

Caruana, R., & Niculescu-Mizil, A. (2006). *An empirical comparison of supervised learning algorithms.* Paper presented at the Proceedings of the 23rd international conference on Machine learning.

Carvalho, D., & Cruz, R. Big data and machine learning in health. *European Journal of Public Health, 30*(Supplement_2). doi:10.1093/eurpub/ckaa040.030

Carvalho, D. V., Pereira, E. M., & Cardoso, J. S. Machine Learning Interpretability: A Survey on Methods and Metrics. *Electronics, 8*(8), 832. doi:10.3390/electronics8080832

Caton, S., & Haas, C. (2024). Fairness in machine learning: A survey. *ACM Computing Surveys, 56*(7), 1-38.

Caturelli, E., Giacobbe, A., Facciorusso, D., Bisceglia, M., Villani, M. R., Siena, D. A., . . . Andriulli, A. (1996). Percutaneous biopsy in diffuse liver disease: increasing diagnostic yield and decreasing complication rate by routine ultrasound assessment of puncture site. *American Journal of Gastroenterology (Springer Nature), 91*(7).

Cawley, G. C. (2012). Over-Fitting in Model Selection and Its Avoidance. In *Lecture Notes in Computer Science* (pp. 1-1): Springer Berlin Heidelberg.

Chakravarthy, A. D., Bonthu, S., Chen, Z., & Zhu, Q. (2019/12//). *Predictive Models with Resampling: A Comparative Study of Machine Lear ning Algorithms and their Performances on Handling Imbalanced Datasets*.

Chandran, N. (2023). Security and Privacy in Machine Learning. In *Lecture Notes in Computer Science* (pp. 229-248): Springer Nature Switzerland.

Chandrashekar, G., & Sahin, F. (2014). A survey on feature selection methods. *Computers & electrical engineering, 40*(1), 16-28.

Chang, C.-H., Ferris, D. L., Johnson, R. E., Rosen, C. C., & Tan, J. A. Core Self-Evaluations. *Journal of Management, 38*(1), 81-128. doi:10.1177/0149206311419661

Chang, C.-W., & Dinh, N. T. Classification of machine learning frameworks for data-driven thermal fluid models. *International Journal of Thermal Sciences, 135*, 559-579. doi:10.1016/j.ijthermalsci.2018.09.002

Changyu, D., Xu, J., Colton, R., Jian-yu, Z., & Wei, L. Integrating Machine Learning with Human Knowledge. *iScience*. doi:10.1016/j.isci.2020.101656

Chantima, B., & S, S. Similar Cluster recommendation of Product Purchases by Pages liked Ana lysis. *European Conference on Artificial Intelligence*. doi:10.1109/ECAI.2018.8679027

Chapel, M.-N., & Bouwmans, T. (2020). Moving objects detection with a moving camera: A comprehensive review. *Computer science review, 38*, 100310.

Chatterjee, S., & Zielinski, P. (2022). On the generalization mystery in deep learning. *arXiv preprint arXiv:2203.10036*.

Chattopadhyay, P., Balaji, Y., & Hoffman, J. (2020). Learning to Balance Specificity and Invariance for In and Out of Domai n Generalization. In *Lecture Notes in Computer Science* (pp. 301-318): Springer International Publishing.

Chawathe, S. S. (2020). *Diagnostic classification using hepatitis C tests.* Paper presented at the 2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS).

Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: synthetic minority over-sampling technique. *Journal of Artificial Intelligence Research, 16*, 321-357.

Chefer, H., Gur, S., & Wolf, L. (2021). *Transformer interpretability beyond attention visualization.* Paper presented at the Proceedings of the IEEE/CVF conference on computer vision and pattern recognition.

Chellapilla, K., Puri, S., & Simard, P. (2006). *High performance convolutional neural networks for document processing.* Paper presented at the Tenth international workshop on frontiers in handwriting recognition.

Chen, C., Zhao, L., Bian, J., Xing, C., & Liu, T.-Y. (2019/7/25/). *Investment Behaviors Can Tell What Inside*.

Chen, D., & Zhao, H. (2012). *Data security and privacy protection issues in cloud computing.* Paper presented at the 2012 international conference on computer science and electronics engineering.

Chen, G., Choi, W., Yu, X., Han, T., & Chandraker, M. (2017). Learning efficient object detection models with knowledge distillation. *Advances in Neural Information Processing Systems, 30*.

Chen, J., & Ran, X. (2019). Deep learning with edge computing: A review. *Proceedings of the IEEE, 107*(8), 1655-1674.

Chen, L., Minjia, H., Mahboob, Q., Saleh, A., & Y, M. Capturing Temporal Dynamics of Users' Preferences from Purchase Histor y Big Data for Recommendation System. *2018 IEEE International Conference on Big Data (Big Data)*. doi:10.1109/BigData.2018.8622411

Chen, M. C., & Henschen, L. J. (1985). On the use and internal structure of logic-based decision support systems. *Decision Support Systems, 1*(3), 205-219.

Chen, T., & Guestrin, C. (2016). *Xgboost: A scalable tree boosting system.* Paper presented at the Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining.

Chen, T., Li, M., Li, Y., Lin, M., Wang, N., Wang, M., . . . Zhang, Z. (2015). Mxnet:

A flexible and efficient machine learning library for heterogeneous distributed systems. *arXiv preprint arXiv:1512.01274*.

Chen, V., Bhatt, U., Heidari, H., Weller, A., & Talwalkar, A. Perspectives on incorporating expert feedback into model updates. *Patterns, 4*(7), 100780. doi:10.1016/j.patter.2023.100780

Chen, X., Singh, M. M., & Geyer, P. Utilizing domain knowledge: Robust machine learning for building energ y performance prediction with small, inconsistent datasets. *Knowledge-Based Systems, 294*, 111774. doi:10.1016/j.knosys.2024.111774

Chen, Y., Li, C., Ghamisi, P., Jia, X., & Gu, Y. (2017). Deep fusion of remote sensing data for accurate classification. *IEEE Geoscience and Remote Sensing Letters, 14*(8), 1253-1257.

Chen, Z., Niu, W., Wu, C., Zhang, L., & Wang, Y. (2021/5/14/). *Near Real-time Situation Awareness and Anomaly Detection for Complex R ailway Environment*.

Chetlur, S., Woolley, C., Vandermersch, P., Cohen, J., Tran, J., Catanzaro, B., & Shelhamer, E. (2014). cudnn: Efficient primitives for deep learning. *arXiv preprint arXiv:1410.0759*.

Chiara, B., Federica, R., & Laura, P. Detection and classification of sensor anomalies for simulating urban traffic scenarios. *Cluster Computing*. doi:10.1007/s10586-021-03445-7

Chicco, D., & Jurman, G. (2021). An ensemble learning approach for enhanced classification of patients with hepatitis and cirrhosis. *IEEE Access, 9*, 24485-24498.

China Academy of Information and Communications Technology (CAICT). (2021a). White Paper on China's Big Data.

China Academy of Information and Communications Technology (CAICT). (2021b). White Paper on China's Computing Power Development Index.

Cho, J. H., & Hariharan, B. (2019). *On the efficacy of knowledge distillation.* Paper presented at the Proceedings of the IEEE/CVF international conference on computer vision.

Cho, M., & Brand, D. (2017). *MEC: memory-efficient convolution for deep neural network.* Paper presented at the International Conference on Machine Learning.

Choi, E., & Lee, C. (2003). Feature extraction based on the Bhattacharyya distance. *Pattern Recognition, 36*(8), 1703-1709.

Chong, Z., & R, P. Anomaly Detection with Robust Deep Autoencoders. *Knowledge Discovery and Data Mining*. doi:10.1145/3097983.3098052

Choudhury, Z. H. BIOMETRICS SECURITY BASED ON FACE RECOGNITION. doi:10.31219/osf.io/75zqr

Chowdhary, K. (2020). Natural language processing. *Fundamentals of artificial intelligence*, 603-649.

Chowdhury, P., & Sinha, B. B. Evaluating the Effectiveness of Collaborative Filtering Similarity Mea sures: A Comprehensive Review. *Procedia Computer Science, 235*, 2641-2650. doi:10.1016/j.procs.2024.04.249

Christoffersen, P., & Jacobs, K. (2004). The importance of the loss function in option valuation. *Journal of Financial Economics, 72*(2), 291-318.

Christoph, M., Giuseppe, C., & B, B. Quantifying Interpretability of Arbitrary Machine Learning Models Thro ugh Functional Decomposition. *arXiv.org*.

Christopher, M. C., & N, W. Embedding domain knowledge for machine learning of complex material sy stems. *MRS Communications*. doi:10.1557/MRC.2019.90

Chua, T.-S. (2016/10/16/). *Beyond Language and Vision, Towards Truly Multimedia Integration*.

Chuan-Kang, T. Quest for the Balance of AI and Privacy [Editor's Remarks]. *IEEE Computational Intelligence Magazine*. doi:10.1109/mci.2022.3180649

Chum, O., & Matas, J. (2008). Optimal randomized RANSAC. *IEEE transactions on pattern analysis and machine intelligence, 30*(8), 1472-1482.

Chum, O., Matas, J., & Kittler, J. (2003). *Locally optimized RANSAC.* Paper presented at the Pattern Recognition: 25th DAGM Symposium, Magdeburg, Germany, September 10-12, 2003. Proceedings 25.

Chung, J., Gulcehre, C., Cho, K., & Bengio, Y. (2014). Empirical evaluation of gated recurrent neural networks on sequence modeling. *arXiv preprint arXiv:1412.3555*.

Chunlei, C., Peng, Z., Huixiang, Z., Jiangyan, D., Yugen, Y., Huihui, Z., & Yonghui, Z. Deep Learning on Computational-Resource-Limited Platforms: A Survey. *Mobile Information Systems*. doi:10.1155/2020/8454327

Ciobanu-Caraus, O., Aicher, A., Kernbach, J. M., Regli, L., Serra, C., & Staartjes, V. E. A critical moment in machine learning in medicine: on reproducible and interpretable learning. *Acta Neurochirurgica, 166*(1). doi:10.1007/s00701-024-05892-8

Clarke, B., Fokoue, E., & Zhang, H. H. (2009). *Principles and theory for data mining and machine learning*: Springer.

Cleveland, M., Robertson, J. L., & Volk, V. Helping or hindering: Environmental locus of control, subjective enabl ers and constraints, and pro-environmental behaviors. *Journal of Cleaner Production, 249*, 119394. doi:10.1016/j.jclepro.2019.119394

Clouqueur, T., Ramanathan, P., Saluja, K. K., & Wang, K.-C. (2001). *Value-fusion versus decision-fusion for fault-tolerance in collaborative target detection in sensor networks.* Paper presented at the Proceedings of Fourth International Conference on Information Fusion.

Cockburn, I., Henderson, R., & Stern, S. *The Impact of Artificial Intelligence on Innovation*. Retrieved from http://dx.doi.org/10.3386/W24449

Congcong, L., Parikh, D., & Tsuhan, C. (2012/6//). *Automatic discovery of groups of objects for scene understanding*.

Connor, I., S, H., & H, H. Energy-efficient Application Resource Scheduling using Machine Learnin g Classifiers. *International Conference on Parallel Processing*. doi:10.1145/3225058.3225088

Cooley, J., & Winograd, S. (1980). *A limited range discrete Fourier transform algorithm.* Paper presented at the ICASSP'80. IEEE International Conference on Acoustics, Speech, and Signal Processing.

Correia, J. L., Pereira, J. A., Mello, R., Garcia, A., Fonseca, B., Ribeiro, M., . . . Tiengo, W. (2020/12//). *Brazilian Data Scientists: Revealing their Challenges and Practices on Machine Learning Model Development*.

Cortes, C., & Mohri, M. (2014). Domain adaptation and sample bias correction theory and algorithm for regression. *Theoretical Computer Science, 519*, 103-126.

Cortes, C., Mohri, M., Gonzalvo, J., & Storcheus, D. (2020). Agnostic learning with multiple objectives. *Advances in Neural Information Processing Systems, 33*, 20485-20495.

Cortes, C., & Vapnik, V. (1995). Support-vector networks. *Machine learning, 20*(3), 273-297.

Countdown, N. (2022). NCD Countdown 2030: efficient pathways and strategic investments to accelerate progress towards the Sustainable Development Goal target 3.4 in

low-income and middle-income countries. *Lancet (London, England), 399*(10331), 1266.

Cse Assistant Professor, P. D. S. E. n. C. THE REAL TIME HIGH PRECISION CRIMINAL FACE RECOGNITION FOR ATM SECURIT Y IN DEEP LEARNING. In *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGE MENT*: Indospace Publications.

Cummings, M. L. M., & Stimpson, A. Identifying Critical Contextual Design Cues Through a Machine Learning Approach. *Ai Magazine, 40*(4), 28-39. doi:10.1609/aimag.v40i4.4811

Cummiskey, B. M., & Baer, M. Bounded creativity: A theory of the effects of constraints on the prod uction of new ideas. *Academy of Management Proceedings, 2018*(1), 15243. doi:10.5465/ambpp.2018.257

Cunningham, P., Cord, M., & Delany, S. J. (2008). Supervised learning. In *Machine learning techniques for multimedia* (pp. 21-49): Springer.

D, F., J, R., & R, S. Oxford Handbook of Psychological Situations.

D, G., M, L., A, Y., Faegheh, H., & Robert, J. v. W. Get a Human-In-The-Loop: Feature Engineering via Interactive Visualiza tions. *IAL@PKDD/ECML*.

D, K. G. An Overview of Artificial Intelligence and Also Potential Security and Privacy Risks Using Machine Learning.

D, M., Cyril, d. B., Johannes, B., A, P., M, V., & Yves-Alexandre, d. M. Improving individual predictions using social networks assortativity. *Workshop on Self-Organizing Maps*. doi:10.1109/WSOM.2017.8020023

D, O., Dunja, V., & Nikola, K. Unlocking Automated Machine Learning Efficiency: Meta-Learning Dynamic s in Social Sciences for Education and Business Data. *TEM Journal*. doi:10.18421/tem131-82

D'Hondt, E., Ashby, T. J., Chakroun, I., Koninckx, T., & Wuyts, R. Identifying and evaluating barriers for the implementation of machine learning in the intensive care unit. *Communications Medicine, 2*(1). doi:10.1038/s43856-022-00225-1

Da Silva, I. N., Hernane Spatti, D., Andrade Flauzino, R., Liboni, L. H. B., dos Reis Alves, S. F., da Silva, I. N., . . . dos Reis Alves, S. F. (2017). *Artificial neural network architectures and training processes*: Springer.

Dahake, P. S., Mohare, R. V., & Somani, N. (2023/8/18/). *Exploring Machine Learning's Potential in Predicting Consumer Behavior for Captivating Marketing*.

Dai, W., Jin, O., Xue, G.-R., Yang, Q., & Yu, Y. (2009). *Eigentransfer: a unified framework for transfer learning.* Paper presented at the Proceedings of the 26th Annual International Conference on Machine Learning.

Dalal, A., Antoine, C., & A, V. L. Adapting Requirements Models to Varying Environments. *International Conference on Software Engineering*. doi:10.1145/3377811.3380927

Daniel, L., Brenton, L., & Mino, D. R. Towards Adversarial Reasoning in Statistical Relational Domains. *StarAI@AAAI*.

Daniels, Z. A., Frank, L. D., Menart, C., Raymer, M., & Hitzler, P. (2020/4/21/). *A framework for explainable deep neural models using external knowledg e graphs*.

Daniels, Z. A., & Metaxas, D. N. (2020). Active Scene Classification via Dynamically Learning Prototypical View s. In *Lecture Notes in Computer Science* (pp. 179-187): Springer International Publishing.

Danijela, R.-D., Marten, F., & K, M. A Review of Vision-Based On-Board Obstacle Detection and Distance Esti mation in Railways. *Italian National Conference on Sensors*.

doi:10.3390/s21103452

Darthy, R., & Britto, P. Assessing The Performance Of Advanced Object Detection Techniques For Autonomous Cars. *2023 International Conference on Networking and Communications (ICNWC)*. doi:10.1109/ICNWC57852.2023.10127360

Das, D., & Lee, C. G. (2018). Sample-to-sample correspondence for unsupervised domain adaptation. *Engineering Applications of Artificial Intelligence, 73*, 80-91.

Dasarathy, B. V. (1994). *Decision fusion* (Vol. 1994): IEEE Computer Society Press Los Alamitos.

David, A.-M., & T, J. Towards Robust Interpretability with Self-Explaining Neural Networks. *Neural Information Processing Systems*.

de Aguiar, E. J., Traina, C., Jr., & Traina, A. J. M. Security and Privacy in Machine Learning for Health Systems: Strategie s and Challenges. *Yearbook of Medical Informatics, 32*(01), 269-281. doi:10.1055/s-0043-1768731

De Maesschalck, R., Jouan-Rimbaud, D., & Massart, D. L. (2000). The mahalanobis distance. *Chemometrics and intelligent laboratory systems, 50*(1), 1-18.

Deep Learning on Edge. *Smart Systems Design, Applications, and Challenges*. doi:10.4018/978-1-7998-2112-0.ch002

Deepika, K., & Seema, S. (2016). *Predictive analytics to prevent and control chronic diseases.* Paper presented at the 2016 2nd international conference on applied and theoretical computing and communication technology (iCATccT).

Dehghani, M., Azarbonyad, H., Kamps, J., & Marx, M. (2016/3/13/). *Generalized Group Profiling for Content Customization*.

Deldjoo, Y., Bellogin, A., & Di Noia, T. Explaining recommender systems fairness and accuracy through the lens of data characteristics. *Information Processing & Management, 58*(5), 102662. doi:10.1016/j.ipm.2021.102662

Deng, J., Dong, W., Socher, R., Li, L.-J., Li, K., & Fei-Fei, L. (2009). *Imagenet: A large-scale hierarchical image database.* Paper presented at the 2009 IEEE conference on computer vision and pattern recognition.

Deng, Z., Choi, K.-S., Jiang, Y., & Wang, S. (2014). Generalized hidden-mapping ridge regression, knowledge-leveraged inductive transfer learning for neural networks, fuzzy systems and kernel methods. *IEEE transactions on cybernetics, 44*(12), 2585-2599.

Denzin, N. K., & Lincoln, Y. S. (2011). *The Sage handbook of qualitative research*: sage.

Derpanis, K. G. (2010). Overview of the RANSAC Algorithm. *Image Rochester NY, 4*(1), 2-3.

Detrano, R. (1988). *Cleveland dataset*. Retrieved from: https://archive.ics.uci.edu/ml/machine-learning-databases/heart-disease/processed.cleveland.data

Dey, R., & Salem, F. M. (2017). *Gate-variants of gated recurrent unit (GRU) neural networks.* Paper presented at the 2017 IEEE 60th international midwest symposium on circuits and systems (MWSCAS).

Dias, P., Tian, Y., Newsam, S., Tsaris, A., Hinkle, J., & Lunga, D. Model Assumptions and Data Characteristics: Impacts on Domain Adaptati on in Building Segmentation. *IEEE Transactions on Geoscience and Remote Sensing, 60*, 1-18. doi:10.1109/tgrs.2022.3175387

Dietterich, T. G., & Michalski, R. S. (1983). A comparative review of selected methods for learning from examples. *Machine learning*, 41-81.

Dietz, L. W., Sánchez, P., & Bellogín, A. Understanding the Influence of Data Characteristics on the Performance of Point-of-Interest Recommendation Algorithms. *arXiv.org*. doi:10.48550/ARXIV.2311.07229

Dimitriadis, S., & Goumopoulos, C. (2008/8//). *Applying Machine Learning to Extract New Knowledge in Precision Agricu lture Applications*.

Din, J. W. Mining of Massive Datasets.

Ding, C., Guo, Z., Rudin, C., Xiao, R., Nahab, F. B., & Hu, X. Reconsideration on evaluation of machine learning models in continuous monitoring using wearables. *arXiv.org*. doi:10.48550/ARXIV.2312.02300

Ding, X., Yang, F., & Ma, F. An efficient model selection for linear discriminant function-based re cursive feature elimination. *Journal of Biomedical Informatics, 129*, 104070. doi:10.1016/j.jbi.2022.104070

Ditzler, G., & Polikar, R. (2011/4//). *Hellinger distance based drift detection for nonstationary environment s*.

Ditzler, G., Roveri, M., Alippi, C., & Polikar, R. Learning in Nonstationary Environments: A Survey. *IEEE Computational Intelligence Magazine, 10*(4), 12-25. doi:10.1109/mci.2015.2471196

Dixon, S., Keshavamurthy, R., Farber, D. H., Stevens, A., Pazdernik, K. T., & Charles, L. E. A Comparison of Infectious Disease Forecasting Methods across Location s, Diseases, and Time. *Pathogens, 11*(2), 185. doi:10.3390/pathogens11020185

Djamba, Y. K. (2002). Social research methods: Qualitative and quantitative approaches. *Teaching Sociology, 30*(3), 380.

Djerioui, M., Brik, Y., Ladjal, M., & Attallah, B. (2019a). Neighborhood component analysis and support vector machines for heart disease prediction.

Djerioui, M., Brik, Y., Ladjal, M., & Attallah, B. (2019b). Neighborhood component analysis and support vector machines for heart disease prediction. *Ingénierie des Systèmes d Inf., 24*(6), 591-595.

Doctoral Student, K. G. S. o. I. S. P. N. U. Y.-r. N. B., Doctoral Student, K. G. S. o. I. S. P. N. U. Y.-r. N. B., Doctoral Student, K. G. S. o. I. S. P. N. U. Y.-r. N. B., Doctoral Student, K. G. S. o. I. S. P. N. U. Y.-r. N. B., & Professor, K. D. o. B. P. N. U. Y.-r. N. B. The Effects of Facial Recognition Payment Systems on Intention to Use in China. In *Journal of Advanced Researches and Reports*: Global Vision Press.

Dodge, Y. (2003). *The Oxford dictionary of statistical terms*: Oxford University Press, USA.

Dodge, Y. (2008). *The concise encyclopedia of statistics*: Springer Science & Business Media.

Dolly, S., & Andy, D. P. Deep Learning Model Reuse and Composition in Knowledge Centric Network ing. *International Conference on Computer Communications and Networks*. doi:10.1109/ICCCN49398.2020.9209668

Dong, D., & Shaowen, H. Random Under-Sampling Ensemble Methods for Highly Imbalanced Rare Dise ase Classification.

Dong, X. L., & Rekatsinas, T. Data integration and machine learning. *Proceedings of the VLDB Endowment, 11*(12), 2094-2097. doi:10.14778/3229863.3229876

Dong, Y., Tang, J., & Zhang, Z. (2022). *Integrated Machine Learning Approaches for E-commerce Customer Behavio r Prediction*.

Donini, M., Oneto, L., Ben-David, S., Shawe-Taylor, J. S., & Pontil, M. (2018). Empirical risk minimization under fairness constraints. *Advances in Neural Information*

*Processing Systems, 31*.

Dorraki, M., Liao, Z., Abbott, D., Psaltis, P. J., Baker, E., Bidargaddi, N., . . . Verjans, J. W. IMPROVING CARDIOVASCULAR DISEASE RISK PREDICTION WITH MACHINE LEARNING USING MENTAL HEALTH DATA: A PROSPECTIVE UK BIOBANK STUDY. *medRxiv*. doi:10.1101/2022.10.23.22281428

Doshi-Velez, F., & Kim, B. (2018). Considerations for evaluation and generalization in interpretable machine learning. *Explainable and interpretable models in computer vision and machine learning*, 3-17.

Dosovitskiy, A., Ros, G., Codevilla, F., Lopez, A., & Koltun, V. (2017). *CARLA: An open urban driving simulator.* Paper presented at the Conference on robot learning.

Doyle, O. M., Leavitt, N., & Rigg, J. A. Finding undiagnosed patients with hepatitis C infection: an applicatio n of artificial intelligence to patient claims data. *Scientific Reports, 10*(1). doi:10.1038/s41598-020-67013-6

Dr, J. R., Raja, K., Dr, A. K., Dr, A. M. P., Dr, V. D. J., P, S., & Vinit, K. Transparency in Algorithmic Decision-making: Interpretable Models for Ethical Accountability. *E3S Web of Conferences*. doi:10.1051/e3sconf/202449102041

Drabiak, K., Kyzer, S., Nemov, V., & El Naqa, I. AI and machine learning ethics, law, diversity, and global impact. *The British Journal of Radiology, 96*(1150). doi:10.1259/bjr.20220934

Dragomir, S. S. (2013). Some reverses of the Jensen inequality with applications. *Bulletin of the Australian Mathematical Society, 87*(2), 177-194.

Draschkow, D., & Võ, M. L. H. Scene grammar shapes the way we interact with objects, strengthens mem ories, and speeds search. *Scientific Reports, 7*(1). doi:10.1038/s41598-017-16739-x

Duboue, P. The Art of Feature Engineering. doi:10.1017/9781108671682

Duddu, V., Szyller, S., & Asokan, N. SoK: Unintended Interactions among Machine Learning Defenses and Risks. *arXiv.org*. doi:10.48550/ARXIV.2312.04542

Ebbehoj, A., Thunbo, M., Andersen, O. E., Glindtvad, M. V., & Hulman, A. Transfer learning for non-image data in clinical research: a scoping r eview. *medRxiv*. doi:10.1101/2021.10.01.21264290

Edeh, M. O., Dalal, S., Dhaou, I. B., Agubosim, C. C., Umoke, C. C., Richard-Nnabu, N. E., & Dahiya, N. (2022). Artificial intelligence-based ensemble learning model for prediction of hepatitis C disease. *Frontiers in Public Health, 10*, 892371.

Eduardo, A., Omar, Y. A.-J., M, D., Saber, F., David, O., & A, M. A Survey on 3D Object Detection Methods for Autonomous Driving Applica tions. *IEEE transactions on intelligent transportation systems (Print)*. doi:10.1109/TITS.2019.2892405

Ekstrand, M. D., & Willemsen, M. C. (2016/9/7/). *Behaviorism is Not Enough*.

El-Bialy, R., Salamay, M. A., Karam, O. H., & Khalifa, M. E. (2015). Feature analysis of coronary artery heart disease data sets. *Procedia Computer Science, 65*, 459-468.

El Shawi, R., Sherif, Y., Al-Mallah, M., & Sakr, S. (2019/6//). *Interpretability in HealthCare A Comparative Study of Local Machine Le arning Interpretability Techniques*.

Emmert-Streib, F., Yang, Z., Feng, H., Tripathi, S., & Dehmer, M. (2020). An introductory review of deep learning for prediction models with big data. *Frontiers in Artificial Intelligence, 3*, 4.

Erickson, N., Mueller, J., Shirkov, A., Zhang, H., Larroy, P., Li, M., & Smola, A. (2020). Autogluon-tabular: Robust and accurate automl for structured data. *arXiv preprint arXiv:2003.06505*.

Esan, O. A., Ngwira, S. M., & Osunmakinde, I. O. (2013/8//). *Bimodal biometrics for financial infrastructure security*.

Esther, R., Theodora, W., B, R., & Michael, I. J. Representation Matters: Assessing the Importance of Subgroup Allocatio ns in Training Data. *International Conference on Machine Learning*.

F, T., Suhel, H., Firuz, K., & Amanda, G. Data imbalance in classification: Experimental evaluation. *Information Sciences*. doi:10.1016/j.ins.2019.11.004

Fabian, H., P, L., Harish, M., Akke, S., & Christian, S. Obstacle detection on rail-tracks: Study on situations for requirement specification. *Transportation Research Procedia*. doi:10.1016/j.trpro.2023.11.498

Fabio, T., & C, A. Data Augmentation Using GANs. *arXiv.org*.

Fan, J., Han, F., & Liu, H. Challenges of Big Data analysis. *National science review, 1*(2), 293-314. doi:10.1093/nsr/nwt032

Fang, G., Annis, I. E., Elston-Lafata, J., & Cykert, S. Applying machine learning to predict real-world individual treatment e ffects: insights from a virtual patient cohort. *Journal of the American Medical Informatics Association, 26*(10), 977-988. doi:10.1093/jamia/ocz036

Farkas, P., Szoke, L., & Aradi, S. (2022/10/12/). *Defining metrics for scenario-based evaluation of autonomous vehicle m odels*.

Farnadi, G., Tang, J., De Cock, M., & Moens, M.-F. (2018/2/2/). *User Profiling through Deep Multimodal Fusion*.

Farrag, A. N., Kamel, A. M., & El-Baraky, I. A. Opportunities and challenges for the application of artificial intelli gence paradigms into the management of endemic viral infections: The e xample of Chronic Hepatitis C Virus. *Reviews in Medical Virology, 34*(2). doi:10.1002/rmv.2514

Farseev, A., Nie, L., Akbari, M., & Chua, T.-S. (2015/6/22/). *Harvesting Multiple Sources for User Profile Learning*.

Farzaneh, K., Zhewen, F., & Vitor, R. C. Improving Robustness on Seasonality-Heavy Multivariate Time Series Ano maly Detection. *arXiv.org*.

Feigenbaum, E. A. (1977). *The art of artificial intelligence. 1. Themes and case studies of knowledge engineering*. Retrieved from

Feigenbaum, E. A. (1979). Themes and case studies of knowledge engineering. *Expert systems in the micro-electronic age*, 3-25.

Feigenbaum, E. A., Buchanan, B. G., & Lederberg, J. (1970). *On generality and problem solving: A case study using the DENDRAL program*. Retrieved from

Feng, D., Haase-Schütz, C., Rosenbaum, L., Hertlein, H., Glaeser, C., Timm, F., . . . Dietmayer, K. (2020). Deep multi-modal object detection and semantic segmentation for autonomous driving: Datasets, methods, and challenges. *IEEE Transactions on Intelligent Transportation Systems, 22*(3), 1341-1360.

Fields, T., Hsieh, G., & Chenou, J. (2019/12//). *Mitigating Drift in Time Series Data with Noise Augmentation*.

Filipe, P., Ruivo, P., & Oliveira, T. Assessing machine learning adoption at the firm level: the moderating effect of the environmental context. *Procedia Computer Science, 219*, 1034-1042. doi:10.1016/j.procs.2023.01.381

Filippo, L. [Risk-based analysis in the handling of sensitive data in the health s ector]. *Giornale Italiano di Nefrologia*.

Firas, B. Towards Robust and Adaptive Machine Learning.

Fischer, L., Ehrlinger, L., Geist, V., Ramler, R., Sobieczky, F., Zellinger, W., & Moser, B. (2020). *Applying AI in practice: key challenges and lessons learned.* Paper presented at the International Cross-Domain Conference for Machine Learning and Knowledge Extraction.

Fisher, A. J., Medaglia, J. D., & Jeronimus, B. F. Lack of group-to-individual generalizability is a threat to human subj ects research. *Proceedings of the National Academy of Sciences, 115*(27). doi:10.1073/pnas.1711978115

Flach, P. (2012). *Machine learning: the art and science of algorithms that make sense of data*: Cambridge university press.

Forough, P.-S., D, G., Jake, M. H., Jennifer, W. V., & Hanna, M. W. Manipulating and Measuring Model Interpretability. *International Conference on Human Factors in Computing Systems*. doi:10.1145/3411764.3445315

Forsyth, D., & Ponce, J. (2011). *Computer vision: A modern approach*: Prentice hall.

Frias, M., Moyano, J. M., Rivero-Juarez, A., Luna, J. M., Camacho, Á., Fardoun, H. M., . . . Ventura, S. Classification Accuracy of Hepatitis C Virus Infection Outcome: Data M ining Approach (Preprint). *Journal of Medical Internet Research*. doi:10.2196/preprints.18766

Frost, M., Doryab, A., & Bardram, J. (2013). *Disease Insights Through Analysis: Using machine learning to provide f eedback in the MONARCA system*.

Fugard, A. J. B., & Stenning, K. Statistical models as cognitive models of individual differences in re asoning. *Argument & Computation, 4*(1), 89-102. doi:10.1080/19462166.2012.674061

Fushiki, T. (2011). Estimation of prediction error by using K-fold cross-validation. *Statistics and Computing, 21*, 137-146.

G, A., & Jingjing, Z. Impact of data characteristics on recommender systems performance. *TMIS*. doi:10.1145/2151163.2151166

G, C. Parallel Computing for Machine Learning in Social Network Analysis. *IEEE International Symposium on Parallel & Distributed Processing, Wor kshops and Phd Forum*. doi:10.1109/IPDPSW.2017.178

G, C., Silvia, A. M., I, P., Anna, L. P., Gian, M. R., & M, A. Enhancing Personal Comfort: a Machine Learning Approach using Physiolo gical and Environmental Signals Measurements. *Measurement*. doi:10.1016/j.measurement.2023.113047

G, F., & S, B. Representation Models and Machine Learning Techniques for Scene Classi ficatio.

Gagne, C. R., & MacEvoy, S. P. Do Simultaneously Viewed Objects Influence Scene Recognition Individua lly or as Groups? Two Perceptual Studies. *PLoS ONE, 9*(8), e102819. doi:10.1371/journal.pone.0102819

Gaidon, A., Wang, Q., Cabon, Y., & Vig, E. (2016). *Virtual worlds as proxy for multi-object tracking analysis.* Paper presented at the Proceedings of the IEEE conference on computer vision and pattern recognition.

Galal, A., & El-Korany, A. (2016). *Enabling Semantic User Context to Enhance Twitter Location Prediction*.

Gan, D., Shen, J., An, B., Xu, M., & Liu, N. (2020). Integrating TANBN with cost sensitive classification algorithm for imbalanced data in medical diagnosis. *Computers & Industrial Engineering, 140*, 106266.

Gao, B., Gouk, H., Yang, Y., & Hospedales, T. (2022). *Loss function learning for*

*domain generalization by implicit gradient.* Paper presented at the International Conference on Machine Learning.

Garcia-Ceja, E., Riegler, M., Kvernberg, A. K., & Torresen, J. User-adaptive models for activity and emotion recognition using deep t ransfer learning and data augmentation. *User Modeling and User-Adapted Interaction, 30*(3), 365-393. doi:10.1007/s11257-019-09248-1

Gardner, S., Golovidov, O., Griffin, J., Koch, P., Thompson, W., Wujek, B., & Xu, Y. (2019/10//). *Constrained Multi-Objective Optimization for Automated Machine Learnin g*.

Gasparini, R., D'Eusanio, A., Borghi, G., Pini, S., Scaglione, G., Calderara, S., . . . Cucchiara, R. (2021/1/10/). *Anomaly Detection, Localization and Classification for Railway Inspect ion*.

Gaurav, S., & Prof, S. S. Advanced Systems for Detecting and Recognizing Traffic Objects. *International Journal of Scientific Research in Computer Science Engin eering and Information Technology*. doi:10.32628/cseit24104111

Gautam, S., & Dey, R. METHODS FOR CLASSIFICATION OF IMBALANCED DATA: A REVIEW. *International Research Journal of Computer Science, 9*(4), 89-95. doi:10.26562/irjcs.2021.v0904.004

Ghany, M. G., Strader, D. B., Thomas, D. L., & Seeff, L. B. (2009). Diagnosis, management, and treatment of hepatitis C: An update#. *Hepatology, 49*(4), 1335-1374.

Ghifary, M., Kleijn, W. B., & Zhang, M. (2014). *Domain adaptive neural networks for object recognition.* Paper presented at the Pacific Rim international conference on artificial intelligence.

Ghotra, B., McIntosh, S., & Hassan, A. E. (2017/5//). *A Large-Scale Study of the Impact of Feature Selection Techniques on D efect Classification Models*.

Gianfrancesco, M. A., Tamang, S., Yazdany, J., & Schmajuk, G. Potential Biases in Machine Learning Algorithms Using Electronic Healt h Record Data. *JAMA Internal Medicine, 178*(11), 1544. doi:10.1001/jamainternmed.2018.3763

Girshick, R. (2015). *Fast r-cnn.* Paper presented at the Proceedings of the IEEE international conference on computer vision.

Giunchiglia, E., Imrie, F., van der Schaar, M., & Lukasiewicz, T. Machine Learning with Requirements: a Manifesto. *arXiv.org*. doi:10.48550/ARXIV.2304.03674

Givoni, M. (2006). Development and impact of the modern high-speed train: A review. *Transport reviews, 26*(5), 593-611.

Glorot, X., Bordes, A., & Bengio, Y. (2011). *Deep sparse rectifier neural networks.* Paper presented at the Proceedings of the fourteenth international conference on artificial intelligence and statistics.

Gohil, V., Dev, S., Upasani, G., Lo, D., Ranganathan, P., & Delimitrou, C. (2024). The Importance of Generalizability in Machine Learning for Systems. *IEEE Computer Architecture Letters*.

Gomes, H. M., Read, J., Bifet, A., Barddal, J. P., & Gama, J. Machine learning for streaming data. *ACM SIGKDD Explorations Newsletter, 21*(2), 6-22. doi:10.1145/3373464.3373470

Gong, Z., Zhong, P., & Hu, W. Diversity in Machine Learning. *IEEE Access, 7*, 64323-64350. doi:10.1109/access.2019.2917620

González, D., & Tansini, L. (2022). Analyzing the Efficiency of Recommender Systems Using Machine Learning. In *Lecture Notes in Networks and Systems* (pp. 692-698): Springer International Publishing.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*: MIT press.

Gorbachev, Y., Fedorov, M., Slavutin, I., Tugarev, A., Fatekhov, M., & Tarkan, Y. (2019). *Openvino deep learning workbench: Comprehensive analysis and tuning of neural networks inference.* Paper presented at the Proceedings of the IEEE/CVF International Conference on Computer Vision Workshops.

Goswami, T., & Roy, U. B. (2020). Classification Accuracy Comparison for Imbalanced Datasets with Its Ba lanced Counterparts Obtained by Different Sampling Techniques. In *Lecture Notes in Electrical Engineering* (pp. 45-54): Springer Nature Singapore.

Gou, J., Yu, B., Maybank, S. J., & Tao, D. (2021). Knowledge distillation: A survey. *International Journal of Computer Vision, 129*(6), 1789-1819.

Gowda, S., Desai, P. B., Hull, V. V., Avinash, A. K., Vernekar, S. N., & Kulkarni, S. S. (2009). A review on laboratory liver function tests. *The Pan african medical journal, 3*.

Graham, M. J., Drake, A. J., Djorgovski, S., Mahabal, A. A., & Donalek, C. (2013). Using conditional entropy to identify periodicity. *Monthly Notices of the Royal Astronomical Society, 434*(3), 2629-2635.

Granziera, E., & Sekhposyan, T. Predicting Relative Forecasting Performance: An Empirical Investigatio n. *SSRN Electronic Journal*. doi:10.2139/ssrn.3280994

Grichi, M., Eghan, E. E., & Adams, B. (2020/9//). *On the Impact of Multi-language Development in Machine Learning Framew orks*.

Groenen, P. J., & Jajuga, K. (2001). Fuzzy clustering with squared Minkowski distances. *Fuzzy Sets and Systems, 120*(2), 227-237.

Gu, W., Foster, K., Shang, J., & Wei, L. (2019). A game-predicting expert system using big data and machine learning. *Expert Systems with Applications, 130*, 293-305.

Guerra-Manzanares, A., Lopez, L. J. L., Maniatakos, M., & Shamout, F. E. (2023). Privacy-Preserving Machine Learning for Healthcare: Open Challenges an d Future Perspectives. In *Lecture Notes in Computer Science* (pp. 25-40): Springer Nature Switzerland.

Guo, L. L., Pfohl, S. R., Fries, J., Posada, J., Fleming, S. L., Aftandilian, C., . . . Sung, L. Systematic Review of Approaches to Preserve Machine Learning Performan ce in the Presence of Temporal Dataset Shift in Clinical Medicine. *Applied Clinical Informatics, 12*(04), 808-815. doi:10.1055/s-0041-1735184

Gupta, S., & Gupta, A. (2019). Dealing with noise problem in machine learning data-sets: A systematic review. *Procedia Computer Science, 161*, 466-474.

Guraya, S. Y., London, N., & Guraya, S. S. (2014). Ethics in medical research. *Journal of Microscopy and Ultrastructure, 2*(3), 121-126.

Guyon, I. (1997). A scaling law for the validation-set training-set size ratio. *AT&T Bell Laboratories, 1*(11).

H, k., H, P., & A, M. A Systematic Review on Imbalanced Data Challenges in Machine Learning. *ACM Computing Surveys*. doi:10.1145/3343440

H, W., Hiromu, U., Foutse, K., Polytechnique, M. e., & Yann-Ga¨el, G. e. e. Machine Learning Architecture and Design Patterns.

Haddouchi, M., & Berrado, A. (2018/10/24/). *Assessing interpretation capacity in Machine Learning*.

Hadil, A., Lefter, S., & Pablo, R. Context-Enriching Feature Selection Method for Industrial Machine Lear ning. *International Conference on Industrial Informatics*. doi:10.1109/INDIN51773.2022.9976131

Hagad, J. L., Moriyama, K., Fukui, K., & Numao, M. (2016). Modeling Work Stress Using Heart Rate and Stress Coping Profiles. In *Lecture Notes in Computer Science* (pp. 108-118): Springer International Publishing.

Hal, A., & Matija, F. The Problem of Behaviour and Preference Manipulation in AI Systems. *SafeAI@AAAI*.

Hall, D., Dayoub, F., Skinner, J., Zhang, H., Miller, D., Corke, P., . . . Sunderhauf, N. (2020/3//). *Probabilistic Object Detection: Definition and Evaluation*.

Hall, P. (1987). On Kullback-Leibler loss and density estimation. *The Annals of Statistics*, 1491-1519.

Hamid, T., Ajay, B., E, A., & Bahram, Z. Challenges and Obstacles Towards Deploying Deep Learning Models on Mob ile Devices. *arXiv.org*.

Han, K., Wang, Y., Chen, H., Chen, X., Guo, J., Liu, Z., . . . Xu, Y. (2022). A survey on vision transformer. *IEEE transactions on pattern analysis and machine intelligence, 45*(1), 87-110.

Han, L., Zheng, T., Xu, L., & Fang, L. (2020). *Occuseg: Occupancy-aware 3d instance segmentation.* Paper presented at the Proceedings of the IEEE/CVF conference on computer vision and pattern recognition.

Han, S., Mao, H., & Dally, W. J. (2015). Deep compression: Compressing deep neural networks with pruning, trained quantization and huffman coding. *arXiv preprint arXiv:1510.00149*.

Hansen, F., & Pedersen, G. K. (2003). Jensen's operator inequality. *Bulletin of the London Mathematical Society, 35*(4), 553-564.

Harari, D., Mars, A., Benoni, H., & Ullman, S. The dynamics of scene understanding. *Journal of Vision, 22*(14), 3555. doi:10.1167/jov.22.14.3555

Harika, A., K, A., Nagpal, A., Singh, D. V., Praveen, & Abdulaali, H. S. (2023/12/1/). *Temporal Data Mining: Uncovering Patterns in Time-Series Data Streams with Machine Learning*.

Harrison, G., Hanson, J., Jacinto, C., Ramirez, J., & Ur, B. (2020). *An empirical study on the perceived fairness of realistic, imperfect machine learning models.* Paper presented at the Proceedings of the 2020 conference on fairness, accountability, and transparency.

Hasan, M., Hanawa, J., Goto, R., Suzuki, R., Fukuda, H., Kuno, Y., & Kobayashi, Y. (2022). LiDAR-based detection, tracking, and property estimation: A contemporary review. *Neurocomputing*.

Hasan, M., & Lu, M. Variance Analysis on Regression Models for Estimating Labor Costs of P refabricated Components. *Journal of Computing in Civil Engineering, 36*(5). doi:10.1061/(asce)cp.1943-5487.0001037

Hashem, S., Esmat, G., Elakel, W., Habashy, S., Raouf, S. A., Elhefnawi, M., . . . ElHefnawi, M. (2017). Comparison of machine learning approaches for prediction of advanced liver fibrosis in chronic hepatitis C patients. *IEEE/ACM transactions on computational biology and bioinformatics, 15*(3), 861-868.

Hashemi, S. H., & Kamps, J. (2017/7/9/). *Where To Go Next?*

Hastie, T., Tibshirani, R., & Friedman, J. (2009). Unsupervised learning. In *The elements of statistical learning* (pp. 485-585): Springer.

Hayashi, S., Prasasti, N., Kanamori, K., & Ohwada, H. (2016). Improving Behavior Prediction Accuracy by Using Machine Learning for A gent-Based Simulation. In *Lecture Notes in Computer Science* (pp. 280-289): Springer Berlin Heidelberg.

He, D., Zou, Z., Chen, Y., Liu, B., Yao, X., & Shan, S. (2021). Obstacle detection of

rail transit based on deep learning. *Measurement, 176*, 109241.

He, K., Zhang, X., Ren, S., & Sun, J. (2016). *Deep residual learning for image recognition.* Paper presented at the Proceedings of the IEEE conference on computer vision and pattern recognition.

Heaton, J. (2016/3//). *An empirical analysis of feature engineering for predictive modeling*.

Hecksteden, A., Kraushaar, J., Scharhag-Rosenberger, F., Theisen, D., Senn, S., & Meyer, T. Individual response to exercise training - a statistical perspective. *Journal of Applied Physiology, 118*(12), 1450-1459. doi:10.1152/japplphysiol.00714.2014

Heidi, L., E, B., Petra, I., C, P., & Sheelagh, C. Seven Guiding Scenarios for Information Visualization Evaluation.

Heinonen, S., Karjalainen, J., & Ruotsalainen, J. (2015). Towards the third industrial revolution. *Finland: Findland Future Research Centre FFRC eBook, 6*, 2015.

Helmstaedter, M. The Mutual Inspirations of Machine Learning and Neuroscience. *Neuron, 86*(1), 25-28. doi:10.1016/j.neuron.2015.03.031

Hemadri, J., & Lakshmish, R. Enhancing Performance of Operationalized Machine Learning Models by An alyzing User Feedback. *International Conference on Image, Video and Signal Processing*. doi:10.1145/3531232.3531261

Hengyu, Z., Yubo, Z., Pingfan, M., Hui, S., Erran, L. L., Tiancheng, L., & Jishen, Z. Driving Scenario Perception-Aware Computing System Design in Autonomou s Vehicles. *ICCD*. doi:10.1109/ICCD50377.2020.00031

Henry, W., C, M., V, J., & Oussama, E.-R. Machine learning-based coreference resolution of concepts in clinical documents. *J. Am. Medical Informatics Assoc.* doi:10.1136/amiajnl-2011-000774

Heo, S., Jeong, S., & Kim, H. RTScale: Sensitivity-Aware Adaptive Image Scaling for Real-Time Object Detection. *Euromicro Conference on Real-Time Systems*. doi:10.4230/LIPICS.ECRTS.2022.2

Herranz, L., Jiang, S., & Li, X. (2016/6//). *Scene Recognition with CNNs: Objects, Scales and Dataset Bias*.

Hershey, J. R., & Olsen, P. A. (2007). *Approximating the Kullback Leibler divergence between Gaussian mixture models.* Paper presented at the 2007 IEEE International Conference on Acoustics, Speech and Signal Processing-ICASSP'07.

Hideaki, T. AIJack: Let's Hijack AI! Security and Privacy Risk Simulator for Machi ne Learning.

Hilbert, M. (2016). Big data for development: A review of promises and challenges. *Development Policy Review, 34*(1), 135-174.

Hill, P. L., Edmonds, G. W., & Jackson, J. J. Pathways Linking Childhood Personality to Later Life Outcomes. *Child Development Perspectives, 13*(2), 116-120. doi:10.1111/cdep.12322

Himel, D. G., & Victor, S. S. A Roadmap to Domain Knowledge Integration in Machine Learning. *2020 IEEE International Conference on Knowledge Graph (ICKG)*. doi:10.1109/ICBK50248.2020.00030

Hintersdorf, D., Struppek, L., & Kersting, K. Balancing Transparency and Risk: The Security and Privacy Risks of Ope n-Source Machine Learning Models. *arXiv.org*. doi:10.48550/ARXIV.2308.09490

Hinton, G., Vinyals, O., & Dean, J. (2015). Distilling the knowledge in a neural network. *arXiv preprint arXiv:1503.02531, 2*(7).

Hinton, G. E. A better way to learn features. *Communications of the ACM, 54*(10), 94-94. doi:10.1145/2001269.2001294

Hinton, G. E., & Salakhutdinov, R. R. (2006). Reducing the dimensionality of data with neural networks. *Science, 313*(5786), 504-507.

Hirschberg, J., & Manning, C. D. (2015). Advances in natural language processing. *Science, 349*(6245), 261-266.

Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural computation, 9*(8), 1735-1780.

Hoens, T. R., Polikar, R., & Chawla, N. V. Learning from streaming data with concept drift and imbalance: an over view. *Progress in Artificial Intelligence, 1*(1), 89-101. doi:10.1007/s13748-011-0008-0

Hofer, P., Roland, M., Schwarz, P., & Mayrhofer, R. (2023). Face to Face with Efficiency: Real-Time Face Recognition Pipelines on Embedded Devices. In *Lecture Notes in Computer Science* (pp. 129-143): Springer Nature Switzerland.

Hoffmann, G., Bietenbeck, A., Lichtinghagen, R., & Klawonn, F. (2018). Using machine learning techniques to generate laboratory diagnostic pathways—a case study. *Journal of Laboratory and Precision Medicine, 3*(6).

Holland, W. W., & Stewart, S. (2018). Screening in disease prevention: what works?

Hopfield, J. J., & Tank, D. W. (1985). "Neural" computation of decisions in optimization problems. *Biological cybernetics, 52*(3), 141-152.

Hopkins, W. G. Individual responses made easy. *Journal of Applied Physiology, 118*(12), 1444-1446. doi:10.1152/japplphysiol.00098.2015

Horkoff, J. (2019/9//). *Non-Functional Requirements for Machine Learning: Challenges and New D irections*.

Hornung, A., Wurm, K. M., Bennewitz, M., Stachniss, C., & Burgard, W. (2013). OctoMap: An efficient probabilistic 3D mapping framework based on octrees. *Autonomous robots, 34*, 189-206.

Howard, A., Sandler, M., Chu, G., Chen, L.-C., Chen, B., Tan, M., . . . Vasudevan, V. (2019). *Searching for mobilenetv3.* Paper presented at the Proceedings of the IEEE/CVF International Conference on Computer Vision.

Howard, A. G., Zhu, M., Chen, B., Kalenichenko, D., Wang, W., Weyand, T., . . . Adam, H. (2017). Mobilenets: Efficient convolutional neural networks for mobile vision applications. *arXiv preprint arXiv:1704.04861*.

Hu, J., Shen, L., & Sun, G. (2018). *Squeeze-and-excitation networks.* Paper presented at the Proceedings of the IEEE conference on computer vision and pattern recognition.

Huang, X., Khetan, A., Cvitkovic, M., & Karnin, Z. (2020). Tabtransformer: Tabular data modeling using contextual embeddings. *arXiv preprint arXiv:2012.06678*.

Huoran, L., & Xuan, L. Mining Device-Specific Apps Usage Patterns from Large-Scale Android Us ers. *arXiv.org*.

Iandola, F. N., Han, S., Moskewicz, M. W., Ashraf, K., Dally, W. J., & Keutzer, K. (2016). SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and< 0.5 MB model size. *arXiv preprint arXiv:1602.07360*.

Ibomoiye, D. M., & Yanxia, S. Performance analysis of cost-sensitive learning methods with applicati on to imbalanced medical data. *Informatics in Medicine Unlocked*. doi:10.1016/j.imu.2021.100690

Inoue, H. (2018). Data augmentation by pairing samples for images classification.

*arXiv preprint arXiv:1801.02929*.

International Data Corporation (IDC) (2021a). Worldwide Global DataSphere Forecast, 2021–2025.

International Data Corporation (IDC) (2021b). Worldwide Semiannual Public Cloud Services Tracker.

Interpretable AI Models for Transparent Decision-Making in Complex Dat a Science Scenarios. *International Journal of Control and Automation*. doi:10.52783/ijca.v13i4.38352

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer, 51*(8), 56-59.

Ishaan, G., & David, L.-P. In Search of Lost Domain Generalization. *International Conference on Learning Representations*.

Izgi, M. C. The concept of privacy in the context of personal health data. *Turkish Journal of Bioethics, 1*(1), 25-37. doi:10.5505/tjob.2014.65375

J, A., & Alexander, W. FPGA based Deterministic Latency Image Acquisition and Processing Syst em for Automated Driving Systems. *International Symposium on Circuits and Systems*. doi:10.1109/ISCAS.2018.8351472

J, A. G. Introduction to Information.

J, G. Deep Learning for Time-Series Analysis. *arXiv.org*.

J, M. D. M., Qiang, Q., Trishul, N., & G, S. Liveness Detection Using Implicit 3D Features. *arXiv.org*.

J, S. Dealing with Data Difficulty Factors While Learning from Imbalanced Da ta. *Challenges in Computational Statistics and Data Mining*. doi:10.1007/978-3-319-18781-5_17

J, W., X, J., Shaoming, X., M, S., & Vipin, K. Integrating Scientific Knowledge with Machine Learning for Engineering and Environmental Systems. *ACM Computing Surveys*. doi:10.1145/3514228

J. Diaz, F., Yeh, H.-W., & de Leon, J. Role of Statistical Random-Effects Linear Models in Personalized Medic ine. *Current Pharmacogenomics and Personalized Medicine, 10*(1), 22-32. doi:10.2174/1875692111201010022

Jacob, M. Learning from evolving data streams. *SciPy*. doi:10.25080/majora-342d178e-025

Jagabathula, S., & Vulcano, G. A Model to Estimate Individual Preferences Using Panel Data. *SSRN Electronic Journal*. doi:10.2139/ssrn.2560994

Jairo, d. S. F. J., & P, P. Performance and model complexity on imbalanced datasets using resampli ng and cost-sensitive algorithms. *Learning with Imbalanced Domains: Theory and Applications*.

Jallouli, M., Lajmi, S., & Amous, I. (2023/5/5/). *Contextualized Recommendation Model Based Socio-Environmental Factors*.

Jamie, R., V, D. S., & A, K. A Cognitive Framework for Object Recognition with Application to Auton omous Vehicles. *Advances in Intelligent Systems and Computing*. doi:10.1007/978-3-030-01174-1_50

Javed, H., Muqeet, H. A., Javed, T., Rehman, A. U., & Sadiq, R. Ethical Frameworks for Machine Learning in Sensitive Healthcare Applic ations. *IEEE Access, 12*, 16233-16254. doi:10.1109/access.2023.3340884

Jenkins, R., & Burton, A. M. 100% Accuracy in Automatic Face Recognition. *Science,*

*319*(5862), 435-435. doi:10.1126/science.1149656

Jeon, H., & Oh, S. Hybrid-Recursive Feature Elimination for Efficient Feature Selection. *Applied Sciences, 10*(9), 3211. doi:10.3390/app10093211

Jeongmin, J., Sung-Ho, H., & H, M. Monocular vision-based object recognition for autonomous vehicle drivi ng in a real driving environment. *International Conference on Ubiquitous Robots and Ambient Intelligence*. doi:10.1109/URAI.2016.7734068

Jia, W., Sun, M., Lian, J., & Hou, S. Feature dimensionality reduction: a review. *Complex & Intelligent Systems, 8*(3), 2663-2693. doi:10.1007/s40747-021-00637-x

Jia, Y. (2014). *Learning semantic image representations at a large scale*: University of California, Berkeley.

Jia, Y., Shelhamer, E., Donahue, J., Karayev, S., Long, J., Girshick, R., . . . Darrell, T. (2014). *Caffe: Convolutional architecture for fast feature embedding.* Paper presented at the Proceedings of the 22nd ACM international conference on Multimedia.

Jiang, P., Ergu, D., Liu, F., Cai, Y., & Ma, B. (2022). A Review of Yolo algorithm developments. *Procedia Computer Science, 199*, 1066-1073.

Jiang, W. Applications of machine learning in neuroscience and inspiration of re inforcement learning for computational neuroscience. *Applied and Computational Engineering, 4*(1), 473-478. doi:10.54254/2755-2721/4/2023308

Jiang, Y., Xue, J., Wang, R., Xia, K., Gu, X., Zhu, J., . . . Qian, P. (2019). Seizure recognition using a novel multitask radial basis function neural network. *Journal of Medical Imaging and Health Informatics, 9*(9), 1865-1870.

Jiang, Z., Wen, H., Han, F., Tang, Y., & Xiong, Y. Data-driven generative design for mass customization: A case study. *Advanced Engineering Informatics, 54*, 101786. doi:10.1016/j.aei.2022.101786

Jin, X.-s. (2018). Key problems faced in high-speed train operation. *China's High-Speed Rail Technology: An International Perspective*, 27-45.

Jin, Y. (2007). *Pareto-based multi-objective machine learning.* Paper presented at the Hybrid Intelligent Systems, International Conference on.

Joachims, T. (1998). *Making large-scale SVM learning practical*. Retrieved from

Johansson, U., Sönströd, C., Norinder, U., & Boström, H. Trade-Off Between Accuracy and Interpretability for Predictive In Silico Modeling. *Future Medicinal Chemistry, 3*(6), 647-663. doi:10.4155/fmc.11.23

Johnson, A. E., Pollard, T. J., Shen, L., Lehman, L.-w. H., Feng, M., Ghassemi, M., . . . Mark, R. G. (2016). MIMIC-III, a freely accessible critical care database. *Scientific data, 3*(1), 1-9.

Jonatan, M. C., M, C., O, K., V, K., & Nguyen, H. Computational Paradox of Deep Learning: A Qualitative Explanation.

Jordan, M. I., & Mitchell, T. M. Machine learning: Trends, perspectives, and prospects. *Science, 349*(6245), 255-260. doi:10.1126/science.aaa8415

Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science, 349*(6245), 255-260.

Joshi, H. Navigating the Intersection of Machine Learning and Healthcare: A Revi ew of Current Applications. *IJARCCE, 11*(10). doi:10.17148/ijarcce.2022.111016

Jubair, S., & Domaratzki, M. Crop genomic selection with deep learning and environmental data: A su rvey. *Frontiers in Artificial Intelligence, 5*. doi:10.3389/frai.2022.1040295

Judge, T. A., & Hurst, C. How the rich (and happy) get richer (and happier): Relationship of cor e self-evaluations to trajectories in attaining work success. *Journal of Applied Psychology, 93*(4), 849-863. doi:10.1037/0021-9010.93.4.849

Jung, S., Son, C., Lee, S., Son, J., Han, J.-J., Kwak, Y., . . . Choi, C. (2019). *Learning to quantize deep networks by optimizing quantization intervals with task loss.* Paper presented at the Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition.

Jung, Y. (2018). Multiple predicting K-fold cross-validation for model selection. *Journal of nonparametric statistics, 30*(1), 197-215.

Junhyoung, O., & K, L. Data De-identification Framework. *Computers, Materials & Continua*. doi:10.32604/cmc.2023.031491

Kaelbling, L. P., Littman, M. L., & Moore, A. W. (1996). Reinforcement learning: A survey. *Journal of artificial intelligence research, 4*, 237-285.

Kalambokis, G., Manousou, P., Vibhakorn, S., Marelli, L., Cholongitas, E., Senzolo, M., . . . Burroughs, A. K. (2007). Transjugular liver biopsy–indications, adequacy, quality of specimens, and complications–a systematic review. *Journal of hepatology, 47*(2), 284-294.

Kandler, C., Zimmermann, J., & McAdams, D. P. Core and Surface Characteristics for the Description and Theory of Per sonality Differences and Development. *European Journal of Personality, 28*(3), 231-243. doi:10.1002/per.1952

Kang, S., Sristi, S., Karachiwala, J., & Hu, Y.-C. (2018/3//). *Detection of Anomaly in Train Speed for Intelligent Railway Systems*.

Karl, F., Pielok, T., Moosbauer, J., Pfisterer, F., Coors, S., Binder, M., . . . Lang, M. (2023). Multi-objective hyperparameter optimization in machine learning—An overview. *ACM Transactions on Evolutionary Learning and Optimization, 3*(4), 1-50.

Karl, F., Pielok, T., Moosbauer, J., Pfisterer, F., Coors, S., Binder, M., . . . Bischl, B. Multi-Objective Hyperparameter Optimization in Machine Learning—An Ove rview. *ACM Transactions on Evolutionary Learning and Optimization, 3*(4), 1-50. doi:10.1145/3610536

Karwa, R., & Honmane, V. (2019). *Building search engine using machine learning technique.* Paper presented at the 2019 International Conference on Intelligent Computing and Control Systems (ICCS).

Katherine, E. B., Steve, T., & Douglas, A. T. A QUEST for Model Assessment: Identifying Difficult Subgroups via Epis temic Uncertainty Quantification. *AMIA ... Annual Symposium proceedings. AMIA Symposium*.

Katona, G., & Bucz, S. (2022/9/11/). *Model of Autonomous Vehicle with Function to Identify Road Signs*.

Katsikopoulos, K. V., & Canellas, M. C. Decoding human behavior with big data? Critical, constructive input fr om the decision sciences. *Ai Magazine, 43*(1), 126-138. doi:10.1002/aaai.12034

Katya, E. Exploring Feature Engineering Strategies for Improving Predictive Mode ls in Data Science. *Research Journal of Computer Systems and Engineering, 4*(2), 201-215. doi:10.52710/rjcse.88

Kaur, N., Kunapuli, G., Joshi, S., Kersting, K., & Natarajan, S. (2020). Neural Networks for Relational Data. In *Lecture Notes in Computer Science* (pp. 62-71): Springer International Publishing.

Ke, G., Meng, Q., Finley, T., Wang, T., Chen, W., Ma, W., . . . Liu, T.-Y. (2017). Lightgbm: A highly efficient gradient boosting decision tree. *Advances in Neural*

*Information Processing Systems, 30*.

Kehrer, J., & Hauser, H. Visualization and Visual Analysis of Multifaceted Scientific Data: A S urvey. *IEEE Transactions on Visualization and Computer Graphics, 19*(3), 495-513. doi:10.1109/tvcg.2012.110

Kenney, N., Jimeng, S., Jianying, H., & Fei, W. Personalized Predictive Modeling and Risk Factor Identification using Patient Similarity. *AMIA Joint Summits on Translational Science proceedings. AMIA Joint Su mmits on Translational Science*.

Kernbach, J. M., & Staartjes, V. E. (2021). Foundations of Machine Learning-Based Clinical Prediction Modeling: Pa rt II—Generalization and Overfitting. In *Acta Neurochirurgica Supplement* (pp. 15-21): Springer International Publishing.

Kerrigan, D., Hullman, J., & Bertini, E. A Survey of Domain Knowledge Elicitation in Applied Machine Learning. *Multimodal Technologies and Interaction, 5*(12), 73. doi:10.3390/mti5120073

Ketcham, M., & Fagfae, N. (2018). The Algorithm for Financial Transactions on Smartphones Using Two-Fact or Authentication Based on Passwords and Face Recognition. In *Advances in Intelligent Systems and Computing* (pp. 223-231): Springer International Publishing.

Kevin, D. A., Shang, G., I, D., E, D., Xiao-Cheng, W., A, S., . . . Hong-Jun, Y. Class imbalance in out-of-distribution datasets: Improving the robustn ess of the TextCNN for the classification of rare cancer types. *Journal of Biomedical Informatics*. doi:10.1016/j.jbi.2021.103957

Khalid, S., Khalil, T., & Nasreen, S. (2014/8//). *A survey of feature selection and feature extraction techniques in mac hine learning*.

Khan, K., Rehman, S. U., Aziz, K., Fong, S., & Sarasvady, S. (2014). *DBSCAN: Past, present and future.* Paper presented at the The fifth international conference on the applications of digital information and web technologies (ICADIWT 2014).

Khan, S., Naseer, M., Hayat, M., Zamir, S. W., Khan, F. S., & Shah, M. (2022). Transformers in vision: A survey. *ACM computing surveys (CSUR), 54*(10s), 1-41.

Khosla, D., Uhlenbrock, R., & Chen, Y. (2017/4//). *Automated scene understanding via fusion of image and object features*.

Ki, H. T., Yuji, R., Young, H. O., Hyunsub, K., & Steven, E. W. Data Cleaning for Accurate, Fair, and Robust Models: A Big Data - AI I ntegration Approach. *DEEM@SIGMOD*. doi:10.1145/3329486.3329493

Kingma, D. P., & Ba, J. (2014). Adam: A method for stochastic optimization. *arXiv preprint arXiv:1412.6980*.

Kittur, P., Pasha, A., Joshi, S., & Kulkarni, V. (2023/12/10/). *A Review on Anti-Spoofing : Face Manipulation and Liveness Detection*.

Klambauer, G., Unterthiner, T., Mayr, A., & Hochreiter, S. (2017). Self-normalizing neural networks. *Advances in Neural Information Processing Systems, 30*.

Klove, T., Lin, T.-T., Tsai, S.-C., & Tzeng, W.-G. (2010). Permutation arrays under the Chebyshev distance. *IEEE Transactions on Information Theory, 56*(6), 2611-2617.

Kohli, A., Shaffer, A., Sherman, A., & Kottilil, S. (2014). Treatment of hepatitis C: a systematic review. *Jama, 312*(6), 631-640.

Kontschieder, P., Fiterau, M., Criminisi, A., & Bulo, S. R. (2015). *Deep neural decision forests.* Paper presented at the Proceedings of the IEEE international conference on computer vision.

Kora, P., Ooi, C. P., Faust, O., Raghavendra, U., Gudigar, A., Chan, W. Y., . . . Rajendra

Acharya, U. Transfer learning techniques for medical image analysis: A review. *Biocybernetics and Biomedical Engineering, 42*(1), 79-107. doi:10.1016/j.bbe.2021.11.004

Kota, T., Shuji, Y., & Tatsuru, H. Boosting Feedback: A Framework for Enhancing Ground Truth Data Collect ion. *BigData Congress [Services Society]*. doi:10.1109/BigData59044.2023.10386658

Kotsiantis, S. B., Zaharakis, I. D., & Pintelas, P. E. (2006). Machine learning: a review of classification and combining techniques. *Artificial Intelligence Review, 26*, 159-190.

Krishnan, S., Magalingam, P., & Ibrahim, R. (2021). Hybrid deep learning model using recurrent neural network and gated recurrent unit for heart disease prediction. *International Journal of Electrical & Computer Engineering (2088-8708), 11*(6).

Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). Imagenet classification with deep convolutional neural networks. *Advances in neural information processing systems, 25*.

Kroll, A., & Soldan, S. On Data-driven Takagi-Sugeno Modeling of Heterogeneous Systems with Mu ltidimensional Membership Functions. *IFAC Proceedings Volumes, 44*(1), 14994-14999. doi:10.3182/20110828-6-it-1002.00266

Ku, J., Mozifian, M., Lee, J., Harakeh, A., & Waslander, S. L. (2018). *Joint 3d proposal generation and object detection from view aggregation.* Paper presented at the 2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS).

Kulvinder, S., & et al. Enhancing Multimodal Information Retrieval Through Integrating Data Mi ning and Deep Learning Techniques. *International Journal on Recent and Innovation Trends in Computing and Communication, 11*(9), 560-569. doi:10.17762/ijritcc.v11i9.8844

Kumar, P., Bhatnagar, R., Gaur, K., & Bhatnagar, A. Classification of Imbalanced Data:Review of Methods and Applications. *IOP Conference Series: Materials Science and Engineering, 1099*(1), 012077. doi:10.1088/1757-899x/1099/1/012077

Kumar, P., Gupta, M. K., Rao, C. R. S., Bhavsingh, M., & Srilakshmi, M. A Comparative Analysis of Collaborative Filtering Similarity Measureme nts for Recommendation Systems. *International Journal on Recent and Innovation Trends in Computing and Communication, 11*(3s), 184-192. doi:10.17762/ijritcc.v11i3s.6180

Kumar, P., & Sharma, M. Data, Machine Learning, and Human Domain Experts: None Is Better than Their Collaboration. *International Journal of Human–Computer Interaction, 38*(14), 1307-1320. doi:10.1080/10447318.2021.2002040

Kumar, R., Singh, U., Sahoo, S., Das, I., & Jha, P. K. (2023). Disease Detection and Risk Prediction System Based Web Application Usi ng Machine Learning. In *Lecture Notes in Computer Science* (pp. 237-249): Springer Nature Switzerland.

Kurebayashi, I., Komuro, N., & Hirai, K. (2021/9/15/). *Testing Machine Learning Models for Individual Emotion Estimation from Indoor Environment Data*.

Kuwajima, H., Yasuoka, H., & Nakae, T. Engineering problems in machine learning systems. *Machine learning, 109*(5), 1103-1126. doi:10.1007/s10994-020-05872-w

Kyriazis, N., & Argyros, A. (2013/6//). *Physically Plausible 3D Scene Tracking: The Single Actor Hypothesis*.

L'Heureux, A., Grolinger, K., Elyamany, H. F., & Capretz, M. A. M. Machine Learning With Big Data: Challenges and Approaches. *IEEE Access, 5*, 7776-7797. doi:10.1109/access.2017.2696365

L, C. Opportunities and Challenges for Resource Management and Machine Learn ing Clusters. *UCC Companion*. doi:10.1145/3368235.3369376

L, G., S, P., J, F., J, P., S, F., Catherine, A., . . . L, S. Systematic Review of Approaches to Preserve Machine Learning Performan ce in the Presence of Temporal Dataset Shift in Clinical Medicine. *Applied Clinical Informatics*. doi:10.1055/s-0041-1735184

Laaksonen, J., & Oja, E. (1996). *Classification with learning k-nearest neighbors.* Paper presented at the Proceedings of international conference on neural networks (ICNN'96).

Lage, I., Chen, E., He, J., Narayanan, M., Kim, B., Gershman, S. J., & Doshi-Velez, F. Human Evaluation of Models Built for Interpretability. *Proceedings of the AAAI Conference on Human Computation and Crowdsourc ing, 7*, 59-67. doi:10.1609/hcomp.v7i1.5280

Lakkaraju, H., & Bastani, O. (2020/2/7/). *"How do I fool you?"*.

Lam, H., Bertini, E., Isenberg, P., Plaisant, C., & Carpendale, S. Empirical Studies in Information Visualization: Seven Scenarios. *IEEE Transactions on Visualization and Computer Graphics, 18*(9), 1520-1536. doi:10.1109/tvcg.2011.279

Larsen, J., Hansen, L. K., Svarer, C., & Ohlsson, M. (1996). *Design and regularization of neural networks: the optimal use of a validation set.* Paper presented at the Neural Networks for Signal Processing VI. Proceedings of the 1996 IEEE Signal Processing Society Workshop.

Latha, C. B. C., & Jeeva, S. C. (2019). Improving the accuracy of prediction of heart disease risk based on ensemble classification techniques. *Informatics in Medicine Unlocked, 16*, 100203.

Lauer, G. M., & Walker, B. D. (2001). Hepatitis C virus infection. *New England journal of medicine, 345*(1), 41-52.

Lavin, A., & Gray, S. (2016). *Fast algorithms for convolutional neural networks.* Paper presented at the Proceedings of the IEEE conference on computer vision and pattern recognition.

Lavrac, N., & Dzeroski, S. (1994). *Inductive Logic Programming.* Paper presented at the WLP.

Le, W., Yong, G., Qi, L., Enhong, C., Bai, L., & Zhenya, H. Modeling Users' Preferences and Social Links in Social Networking Serv ices: A Joint-Evolving Perspective. *AAAI Conference on Artificial Intelligence*. doi:10.1609/aaai.v30i1.9980

LeCun, Y., Denker, J., & Solla, S. (1989). Optimal brain damage. *Advances in neural information processing systems, 2*.

Lee, K., Sood, A., & Craven, M. Understanding Learned Models by Identifying Important Features at the Right Resolution. *Proceedings of the AAAI Conference on Artificial Intelligence, 33*(01), 4155-4163. doi:10.1609/aaai.v33i01.33014155

Lee, S., Hwang, Y., Jin, Y., Ahn, S., & Park, J. Effects of individuality, education, and image on visual attention: An alyzing eye-tracking data using machine learning. *Journal of Eye Movement Research, 12*(2). doi:10.16910/jemr.12.2.4

Lee, W. C. (1990). Estimate of channel capacity in Rayleigh fading environment. *IEEE transactions on Vehicular Technology, 39*(3), 187-189.

Leng, J., Liu, Y., Du, D., Zhang, T., & Quan, P. (2019). Robust obstacle detection and recognition for driver assistance systems. *IEEE Transactions on Intelligent Transportation Systems, 21*(4), 1560-1571.

Leonardo, Y. K., Gabriel, M. P. P., Thomas, C. M. M., Maria, d. F. A., & Prashant, K. Enhancing spatial inference of air pollution using machine learning te chniques with low-cost monitors in data-limited scenarios. *Environmental science: atmospheres*. doi:10.1039/d3ea00126a

Li, D., & Kaewunruen, S. Effect of Extreme Climate on Topology of Railway Prestressed Concrete Sleepers. *Climate, 7*(1), 17. doi:10.3390/cli7010017

Li, D., Yang, Y., Song, Y.-Z., & Hospedales, T. M. (2017). *Deeper, broader and artier domain generalization.* Paper presented at the Proceedings of the IEEE international conference on computer vision.

Li, H., Li, W., Pan, X., Huang, J., Gao, T., Hu, L., . . . Lu, Y. Correlation and redundancy on machine learning performance for chemica l databases. *Journal of Chemometrics, 32*(7). doi:10.1002/cem.3023

Li, J., & Liu, H. Challenges of Feature Selection for Big Data Analytics. *IEEE Intelligent Systems, 32*(2), 9-15. doi:10.1109/mis.2017.38

Li, L., Doroslovački, M., & Loew, M. H. (2020). Approximating the gradient of cross-entropy loss function. *IEEE Access, 8*, 111626-111635.

Li, T.-H. S., Chiu, H.-J., & Kuo, P.-H. (2022). Hepatitis C virus detection model by using random forest, logistic-regression and ABC algorithm. *IEEE Access, 10*, 91045-91058.

Li, Y., Ma, L., Zhong, Z., Liu, F., Chapman, M. A., Cao, D., & Li, J. (2020). Deep learning for lidar point clouds in autonomous driving: A review. *IEEE Transactions on Neural Networks and Learning Systems, 32*(8), 3412-3432.

Li, Y., Mao, H., Girshick, R., & He, K. (2022). *Exploring plain vision transformer backbones for object detection.* Paper presented at the European Conference on Computer Vision.

Li, Y., Yu, A. W., Meng, T., Caine, B., Ngiam, J., Peng, D., . . . Le, Q. V. (2022). *Deepfusion: Lidar-camera deep fusion for multi-modal 3d object detection.* Paper presented at the Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition.

Liao, S.-H. (2005). Expert system methodologies and applications—a decade review from 1995 to 2004. *Expert Systems with Applications, 28*(1), 93-103.

Liberti, L., Lavor, C., Maculan, N., & Mucherino, A. (2014). Euclidean distance geometry and applications. *SIAM review, 56*(1), 3-69.

Lichtinghagen, & Hoffmann, G. *HCV data*: UCI Machine Learning Repository.

Limdi, J., & Hyde, G. (2003). Evaluation of abnormal liver function tests. *Postgraduate medical journal, 79*(932), 307-312.

Lin-lin, Z. A Study on the Impact of Face Recognition Payment System Characteristi cs and Innovation Resistance on Intention to Use: Focusing on Chinese Users. doi:10.17762/TURCOMAT.V12I10.4285

Lin, S., Ji, R., Chen, C., Tao, D., & Luo, J. (2018). Holistic cnn compression via low-rank decomposition with knowledge transfer. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 41*(12), 2889-2905.

Lin, T.-Y., Maire, M., Belongie, S., Hays, J., Perona, P., Ramanan, D., . . . Zitnick, C. L. (2014). *Microsoft coco: Common objects in context.* Paper presented at the Computer Vision–ECCV 2014: 13th European Conference, Zurich, Switzerland, September 6-12, 2014, Proceedings, Part V 13.

Lin, Y., Lv, F., Zhu, S., Yang, M., Cour, T., Yu, K., . . . Zhou, X. (2010). Imagenet classification: fast descriptor coding and large-scale svm training. *Large scale visual recognition challenge*.

Linardatos, P., Papastefanopoulos, V., & Kotsiantis, S. Explainable AI: A Review of Machine Learning Interpretability Methods. *Entropy, 23*(1), 18. doi:10.3390/e23010018

Lincy, M., & Seetha, H. Learning From Imbalanced Data. *Advances in Computer and Electrical Engineering*. doi:10.4018/978-1-5225-2255-3.CH159

Lindeberg, T. (2012). Scale invariant feature transform.

Lisy, V., Jakob, M., Tozicka, J., & Pechoucek, M. (2008/10//). *Utility-based model for classifying adversarial behaviour in multi-age nt systems*.

Littmann, M., Selig, K., Cohen-Lavi, L., Frank, Y., Hönigschmid, P., Kataka, E., . . . Rost, B. Validity of machine learning in biology and medicine increased through collaborations across fields of expertise. *Nature Machine Intelligence, 2*(1), 18-24. doi:10.1038/s42256-019-0139-8

Litzkendorf, S., Frank, M., Babac, A., Rosenfeldt, D., Schauer, F., Hartz, T., & Graf von der Schulenburg, J. M. Use and importance of different information sources among patients wit h rare diseases and their relatives over time: a qualitative study. *BMC Public Health, 20*(1). doi:10.1186/s12889-020-08926-9

Liu, H., Gegov, A., & Cocea, M. (2017). Unified Framework for Control of Machine Learning Tasks Towards Effect ive and Efficient Processing of Big Data. In *Studies in Big Data* (pp. 123-140): Springer International Publishing.

Liu, W., Anguelov, D., Erhan, D., Szegedy, C., Reed, S., Fu, C.-Y., & Berg, A. C. (2016). *Ssd: Single shot multibox detector.* Paper presented at the Computer Vision–ECCV 2016: 14th European Conference, Amsterdam, The Netherlands, October 11–14, 2016, Proceedings, Part I 14.

Liu, Z., Lin, Y., Cao, Y., Hu, H., Wei, Y., Zhang, Z., . . . Guo, B. (2021). *Swin transformer: Hierarchical vision transformer using shifted windows.* Paper presented at the Proceedings of the IEEE/CVF international conference on computer vision.

Liu, Z., Sun, M., Zhou, T., Huang, G., & Darrell, T. (2018). Rethinking the value of network pruning. *arXiv preprint arXiv:1810.05270*.

Long, M., Wang, J., Ding, G., Sun, J., & Yu, P. S. (2013). *Transfer feature learning with joint distribution adaptation.* Paper presented at the Proceedings of the IEEE international conference on computer vision.

Long, X., David, M. G., Sukhwa, H., & Patricia, G. Transfer Learning in Knowledge-Intensive Tasks: A Test in Healthcare T ext Analytics. *Americas Conference on Information Systems*.

Lopes-Ramos, C. M., Quackenbush, J., & DeMeo, D. L. Genome-Wide Sex and Gender Differences in Cancer. *Frontiers in Oncology, 10*. doi:10.3389/fonc.2020.597788

Lowe, G. (2004). Sift-the scale invariant feature transform. *Int. J, 2*(91-110), 2.

Lu, Z. A Theory of Multimodal Learning. *Neural Information Processing Systems*. doi:10.48550/ARXIV.2309.12458

Luc, R., J, H., & Y, d. M. Estimating the success of re-identifications in incomplete datasets us ing generative models. *Nature Communications*. doi:10.1038/s41467-019-10933-3

Lucia, L. S. Building Adaptive Industry Cartridges Using a Semi-supervised Machine Learning Method. *Computer Vision Conference*. doi:10.1007/978-3-030-17795-9_58

Luo, M. C., Nikolopoulou, E., & Gevertz, J. L. From Fitting the Average to Fitting the Individual: A Cautionary Tale for Mathematical Modelers. *Frontiers in Oncology, 12*. doi:10.3389/fonc.2022.793908

Lv, D., Ying, X., Cui, Y., Song, J., Qian, K., & Li, M. (2017). *Research on the technology of LIDAR data processing.* Paper presented at the 2017 First International Conference on Electronics Instrumentation & Information Systems (EIIS).

Lwakatare, L. E., Raj, A., Crnkovic, I., Bosch, J., & Olsson, H. H. (2020). Large-scale machine learning systems in real-world industrial settings: A review of challenges and solutions. *Information and software technology, 127*, 106368.

Lydia, T. L., Sarah, D., Esther, R., Max, S., & Moritz, H. Delayed Impact of Fair Machine Learning. *International Conference on Machine Learning*. doi:10.24963/ijcai.2019/862

M, A., Adrian, B. T., W, C., S, D., S, D.-B., K, G., . . . E, K. Integrating machine learning and multiscale modeling—perspectives, cha llenges, and opportunities in the biological, biomedical, and behavior al sciences. *npj Digital Medicine*. doi:10.1038/s41746-019-0193-y

M, A., & D, P. ADAPT: An Adaptive Machine Learning Framework with Application to Lith ography Hotspot Detection. *Workshop on Machine Learning for CAD*. doi:10.1109/MLCAD52597.2021.9531210

M, A., & Di, W. Machine Learning Pipeline for Reusing Pretrained Models. *International ACM Conference on Management of Emergent Digital EcoSyst ems*. doi:10.1145/3415958.3433054

M, D., & S, S. User based Collaborative Filtering with Temporal Information for Purch ase Data. *International Conference on Knowledge Discovery and Information Retrie val*. doi:10.5220/0004134400550064

M, G. A., K, A., & S, S. A.-R. Intelligent Object Recognition System for Autonomous and Semi-Autonomo us Vehicles. *International Congress on Information and Communication Technology*. doi:10.1109/ICICT52195.2021.9568417

M, G. A., K, A., & S, S. A.-R. Object Recognition System for Autonomous Vehicles Based on PCA and 1D- CNN. *2021 7th International Conference on Contemporary Information Technolo gy and Mathematics (ICCITM)*. doi:10.1109/ICCITM53167.2021.9677676

M, H., & Bernhard, W. Sensor and object recognition technologies for self-driving cars. doi:10.1080/16864360.2017.1419638

M, P., Apostolos, A., Remi, E., A, C., & I, S. A metric suite for evaluating interactive scenarios in video games: an empirical validation. *ACM Symposium on Applied Computing*. doi:10.1145/3341105.3373985

M, P., & G, S. AN ANALYSIS OF PRIVACY RISKS AND DESIGN PRINCIPLES FOR DEVELOPING COUN TERMEASURES IN PRIVACY PRESERVING SENSITIVE DATA PUBLISHING.

M, R., N, M., & F, A. An obstacle detection system for automated trains. *IEEE IV2003 Intelligent Vehicles Symposium. Proceedings (Cat. No.03TH8 683)*. doi:10.1109/IVS.2003.1212905

M, S., & M, A. Object/Obstacles detection system for self-driving cars. *Australian Workshop on Safety Critical Systems and Software*. doi:10.1049/icp.2022.0333

M, S., Milan, B., D, S., Marten, F., Kai, M., Ingo, S., . . . Marjan, D. Toward the Enhancement of Rail Sustainability: Demonstration of a Holi stic Approach to Obstacle Detection in Operational Railway Environment s. *Sustainability*. doi:10.3390/su16072613

M, Z., Michael, S., B, S., & K, S. Detailed 3D Representations for Object Recognition and Modeling. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. doi:10.1109/TPAMI.2013.87

Ma, C., Wang, N., Chen, Q. A., & Shen, C. SlowTrack: Increasing the Latency of Camera-based Perception in Autono mous Driving Using Adversarial Examples. *AAAI Conference on Artificial Intelligence*. doi:10.48550/ARXIV.2312.09520

Ma, N., Zhang, X., Zheng, H.-T., & Sun, J. (2018). *Shufflenet v2: Practical guidelines for efficient cnn architecture design.* Paper presented at the Proceedings of the European conference on computer vision (ECCV).

MacArthur, G. J., van Velzen, E., Palmateer, N., Kimber, J., Pharris, A., Hope, V., . . . Goldberg, D. (2014). Interventions to prevent HIV and hepatitis C in people who inject drugs: a review of reviews to assess evidence of effectiveness. *International Journal of Drug Policy, 25*(1), 34-52.

Maccio, V. J., Chiang, F., & Down, D. G. (2014). Models for Distributed, Large Scale Data Cleaning. In *Lecture Notes in Computer Science* (pp. 369-380): Springer International Publishing.

Machine Learning under Resource Constraints - Volume 3: Applications. *Mach. Learn. under Resour. Constraints Vol. 3*. doi:10.1515/9783110785982

Maedeh, H., Shahin, H., & Hojat, H. Advancing personal thermal comfort prediction: A data-driven framework integrating environmental and occupant dynamics using machine learnin g. *Building and Environment*. doi:10.1016/j.buildenv.2024.111799

Magtibay, K., Fernando, X., & Umapathy, K. (2022). *Enhancement of Physiological Stress Classification using Psychometric Features*.

Mahesh, B. (2020). Machine learning algorithms-a review. *International Journal of Science and Research (IJSR).[Internet], 9*, 381-386.

Mahmood, S., Huebner, M., & Reichenbach, M. (2023). A Design-Space Exploration Framework for Application-Specific Machine Learning Targeting Reconfigurable Computing. In *Lecture Notes in Computer Science* (pp. 371-374): Springer Nature Switzerland.

Mahmoud, A., El-Kilany, A., Ali, F., & Mazen, S. (2020/6/1/). *A Novel Oversampling Technique To Handle Imbalanced Datasets*.

Majd, A., Maram, B. Y., & R, Q. An Object Classification Approach for Autonomous Vehicles Using Machin e Learning Techniques. *World Electric Vehicle Journal*. doi:10.3390/wevj14020041

Makhoul, A., & Harb, H. Data Reduction in Sensor Networks: Performance Evaluation in a Real En vironment. *IEEE Embedded Systems Letters, 9*(4), 101-104. doi:10.1109/les.2017.2749333

Malakar, N. Environmental Intelligence using Machine Learning Applications. *Journal of Nepal Physical Society, 8*(2), 42-47. doi:10.3126/jnphyssoc.v8i2.50148

Malik, M. M. (2020). A hierarchy of limitations in machine learning. *arXiv preprint arXiv:2002.05193*.

Mangos, P. M., & Hulse, N. A. Advances in machine learning applications for scenario intelligence: d eep learning. *Theoretical Issues in Ergonomics Science, 18*(2), 184-198. doi:10.1080/1463922x.2016.1166406

Manias, D. M., Chouman, A., & Shami, A. Model Drift in Dynamic Networks. *IEEE Communications Magazine, 61*(10), 78-84. doi:10.1109/mcom.003.2200306

Mannila, H. (1996). *Data mining: machine learning, statistics, and databases.* Paper presented at the Proceedings of 8th international conference on scientific and statistical data base management.

Manuel, M., Alvaro, C., & S, S. MOPED: A scalable and low latency object recognition and pose estimati on system. *IEEE International Conference on Robotics and Automation*. doi:10.1109/ROBOT.2010.5509801

Manuja, K., & Bhattacharya, A. (2015/3/18/). *Using social connections to improve*

*collaborative filtering*.

Marblestone, A. H., Wayne, G., & Kording, K. P. Toward an Integration of Deep Learning and Neuroscience. *Frontiers in Computational Neuroscience, 10*. doi:10.3389/fncom.2016.00094

Marcinkiewicz, M. A. (1994). Building a large annotated corpus of English: The Penn Treebank. *Using Large Corpora*, 273.

Marcos, M.-G., M, M., José, C. C., Á, C.-G., & M, S. Personalizing Activity Selection in Assistive Social Robots from Expli cit and Implicit User Feedback. *International Journal of Social Robotics*. doi:10.1007/s12369-024-01124-2

Maria, N. N., Konstantina, D., Katia, L. K., & Adamantia, G. P. Machine Learning on Wikipedia Text for the Automatic Identification of Vocational Domains of Significance for Displaced Communities. *International Workshop on Semantic and Social Media Adaptation and Per sonalization*. doi:10.1109/SMAP56125.2022.9941803

Marlena, J. G. Big data at work: dispelling the myths, uncovering the opportunities. *Choice Reviews Online, 51*(11), 51-6260-6251-6260. doi:10.5860/choice.51-6260

Masahiro, S., Hidetaka, I., & Takashi, S. Modeling Individual Users' Responsiveness to Maximize Recommendation I mpact. *User Modeling, Adaptation, and Personalization*. doi:10.1145/2930238.2930259

Masahiro, S., Janmajay, S., S, T., Takashi, S., Qian, Z., & Tomoko, O. Modeling user exposure with recommendation influence. *ACM Symposium on Applied Computing*. doi:10.1145/3341105.3375760

Maturana, D., & Scherer, S. (2015). *Voxnet: A 3d convolutional neural network for real-time object recognition.* Paper presented at the 2015 IEEE/RSJ international conference on intelligent robots and systems (IROS).

Max-Marcel, T., J, J. K., Gwendolyn, M., Christian, H., & Rüdiger, Z. Employing Environmental Data and Machine Learning to Improve Mobile He alth Receptivity. *IEEE Access*. doi:10.1109/ACCESS.2019.2958474

Maxim, B., F, D., & Arnon, S. From US to Domain Models: Recommending Relationships between Entities. *REFSQ Workshops*.

Maximilian, B., F, S., Viktor, G., & Ana, K. Towards A Platform and Benchmark Suite for Model Training on Dynamic D atasets. *EuroMLSys@EuroSys*. doi:10.1145/3578356.3592585

McClelland, J. L., Rumelhart, D. E., & Hinton, G. E. (1986). The appeal of parallel distributed processing. *MIT Press, Cambridge MA*, 3-44.

McGibbon, E., Bornschlegel, K., & Balter, S. (2013). Half a diagnosis: gap in confirming infection among hepatitis C antibody-positive patients. *The American journal of medicine, 126*(8), 718-722.

McInnes, L., Healy, J., & Astels, S. (2017). hdbscan: Hierarchical density based clustering. *J. Open Source Softw., 2*(11), 205.

McKinney, W. (2011). pandas: a foundational Python library for data analysis and statistics. *Python for high performance and scientific computing, 14*(9), 1-9.

Md, Y. A., S, H., Shuxiang, X., & D, F. Machine Learning for Mining Imbalanced Data.

Melis, G., Kočiský, T., & Blunsom, P. (2019). Mogrifier lstm. *arXiv preprint arXiv:1909.01792*.

Mende, H., Frye, M., Vogel, P.-A., Kiroriwal, S., Schmitt, R. H., & Bergs, T. On the importance of domain expertise in feature engineering for predi ctive product quality in

production. *Procedia CIRP, 118*, 1096-1101. doi:10.1016/j.procir.2023.06.188

Menik, S., & Ramaswamy, L. Towards Modular Machine Learning Solution Development: Benefits and Tr ade-offs. *arXiv.org*. doi:10.48550/ARXIV.2301.09753

Meor Yahaya, M. S., & Teo, J. Data augmentation using generative adversarial networks for images and biomarkers in medicine and neuroscience. *Frontiers in Applied Mathematics and Statistics, 9*. doi:10.3389/fams.2023.1162760

Mescheder, L., Oechsle, M., Niemeyer, M., Nowozin, S., & Geiger, A. (2019). *Occupancy networks: Learning 3d reconstruction in function space.* Paper presented at the Proceedings of the IEEE/CVF conference on computer vision and pattern recognition.

Mhou, K., van der Haar, D., & Leung, W. S. (2017/6//). *Face spoof detection using light reflection in moderate to low lightin g*.

Mi, Z., Faen, Z., N, L., Yuanchao, S., Xiao, Z., Biyi, F., . . . Hui, X. Deep Learning in the Era of Edge Computing: Challenges and Opportuniti es. *Fog Computing*. doi:10.1002/9781119551713.ch3

Micallef, L., Sundin, I., Marttinen, P., Ammad-ud-din, M., Peltola, T., Soare, M., . . . Kaski, S. (2017/3/7/). *Interactive Elicitation of Knowledge on Feature Relevance Improves Pre dictions in Small Data Sets*.

Michalski, R. S., & Kodratoff, Y. (1990). Research in machine learning: Recent progress, classification of methods, and future directions. *Machine learning*, 3-30.

Mikołajczyk, A., & Grochowski, M. (2018). *Data augmentation for improving deep learning in image classification problem.* Paper presented at the 2018 international interdisciplinary PhD workshop (IIPhDW).

Milo, T., & Somech, A. (2020). *Automating exploratory data analysis via machine learning: An overview.* Paper presented at the Proceedings of the 2020 ACM SIGMOD international conference on management of data.

Min, W., & Zuosu, J. The Defining Approaches and Practical Paradox of Sensitive Data: An In vestigation of Data Protection Laws in 92 Countries and Regions and 20 0 Data Breaches in the World.

Mingers, J. (1989). An empirical comparison of pruning methods for decision tree induction. *Machine learning, 4*(2), 227-243.

Minsky, M. (1961). Steps toward artificial intelligence. *Proceedings of the IRE, 49*(1), 8-30.

Minsky, M. (1974). A framework for representing knowledge. In: MIT, Cambridge.

Mirza, M. J., Buerkle, C., Jarquin, J., Opitz, M., Oboril, F., Scholl, K.-U., & Bischof, H. (2021/9/19/). *Robustness of Object Detectors in Degrading Weather Conditions*.

Mishra, S., Kumar, R., Tiwari, S. K., & Ranjan, P. Machine learning approaches in the diagnosis of infectious diseases: a review. *Bulletin of Electrical Engineering and Informatics, 11*(6), 3509-3520. doi:10.11591/eei.v11i6.4225

Mishra, S., & Pradhan, R. K. (2023/1/27/). *Analyzing the Impact of Feature Correlation on Classification Acuracy of Machine Learning Model*.

Misra, P., & Siddharth. (2017/5//). *Machine learning and time series: Real world applications*.

Mitchell, T. M. (1997). Machine learning. In: McGraw-hill New York.

Mohammed, R., Rawashdeh, J., & Abdullah, M. (2020/4//). *Machine Learning with Oversampling and Undersampling Techniques: Overv iew Study and Experimental Results*.

Mohandas, D. R., Veena, D. S., Kirubasri, G., Mary, I. T. B., & Udayakumar, D. R.

Federated Learning with Homomorphic Encryption for Ensuring Privacy in Medical Data. *Indian Journal of Information Sources and Services, 14*(2), 17-23. doi:10.51983/ijiss-2024.14.2.03

Mohsen, S., Nima, K., Michael, A. B., & S, B. Traffic Object Detection and Recognition Based on the Attentional Visu al Field of Drivers. *IEEE Transactions on Intelligent Vehicles*. doi:10.1109/TIV.2021.3133849

Molchanov, P., Mallya, A., Tyree, S., Frosio, I., & Kautz, J. (2019). *Importance estimation for neural network pruning.* Paper presented at the Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition.

Molnar, C., Casalicchio, G., & Bischl, B. (2020). Quantifying Model Complexity via Functional Decomposition for Better P ost-hoc Interpretability. In *Communications in Computer and Information Science* (pp. 193-204): Springer International Publishing.

Monmasson, E., Idkhajine, L., Cirstea, M. N., Bahri, I., Tisan, A., & Naouar, M. W. (2011). FPGAs in industrial control applications. *IEEE Transactions on Industrial informatics, 7*(2), 224-243.

Moradi, R., & Groth, K. On the application of transfer learning in prognostics and health mana gement. *Annual Conference of the PHM Society, 12*(1), 8. doi:10.36001/phmconf.2020.v12i1.1300

Morgan, K. P. 3-D VISION FOR OUTDOOR NAVIGATION BY AN AUTONOMOUS VEHICLE.

Mori, M., Shahian, D. M., Huang, C., Li, S.-X., Normand, S.-L. T., Geirsson, A., & Krumholz, H. M. Surgeons: Buyer beware—does “universal” risk prediction model apply to patients universally? *The Journal of Thoracic and Cardiovascular Surgery, 160*(1), 176-179.e172. doi:10.1016/j.jtcvs.2019.11.144

Morik, K., Rahnenführer, J., & Wietfeld, C. (2023). *Machine learning under resource constraints*: De Gruyter.

Moritz, B., Siemsen, E., & Kremer, M. Judgmental Forecasting: Cognitive Reflection and Decision Speed. *Production and Operations Management, 23*(7), 1146-1160. doi:10.1111/poms.12105

Moss, L., Corsar, D., Shaw, M., Piper, I., & Hawthorne, C. Demystifying the Black Box: The Importance of Interpretability of Pred ictive Models in Neurocritical Care. *Neurocritical Care, 37*(S2), 185-191. doi:10.1007/s12028-022-01504-4

Mousavi, M., Shahbazi, N., & Asudeh, A. Data Coverage for Detecting Representation Bias in Image Datasets: A C rowdsourcing Approach. *International Conference on Extending Database Technology*. doi:10.48550/ARXIV.2306.13868

Mueller, J., Shi, X., & Smola, A. (2020). *Faster, simpler, more accurate: practical automated machine learning with tabular, text, and image data.* Paper presented at the Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining.

Muggleton, S., & De Raedt, L. (1994). Inductive logic programming: Theory and methods. *The Journal of Logic Programming, 19*, 629-679.

Muhammad, E. R., Amir, Z., & Ahmad, A. USE OF IMAGE ENHANCEMENT TECHNIQUES FOR IMPROVING REAL TIME FACE RECOG NITION EFFICIENCY ON WEARABLE GADGETS.

Mukamakuza, C. P., Sacharidis, D., & Werthner, H. (2019/6/6/). *The Impact of Social Connections in Personalization*.

Mukherjee, R., Burns, A., Rodden, D., Chang, F., Chaum, M., Garcia, N., . . . Niemz, A. Diagnosis and Management of Hepatitis C Virus Infection. *SLAS Technology, 20*(5),

519-538. doi:10.1177/2211068214563794

Mukkamala, R., Gagnon, J., & Jajodia, S. (2000). Integrating Data Mining Techniques with Intrusion Detection Methods. In *IFIP Advances in Information and Communication Technology* (pp. 33-46): Springer US.

Mumuni, A., & Mumuni, F. Automated data processing and feature engineering for deep learning an d big data applications: A survey. *Journal of Information and Intelligence*. doi:10.1016/j.jiixd.2024.01.002

Murphy, R. R. (2019). *Introduction to AI robotics*: MIT press.

Murray, C. J., Abbafati, C., Abbas, K. M., Abbasi, M., Abbasi-Kangevari, M., Abd-Allah, F., . . . Abolhassani, H. (2020). Five insights from the global burden of disease study 2019. *The Lancet, 396*(10258), 1135-1159.

Murtagh, F. (1991). Multilayer perceptrons for classification and regression. *Neurocomputing, 2*(5-6), 183-197.

N, D., Chadaga, N. B., Singh, H., & N, K. (2022/11/20/). *Empirical Analysis of Sampling Methods on Imbalanced Data*.

N, M., Dr, P. D., & Dr, C. M. A. Environmental Intelligence using Machine Learning Applications. *Journal of Nepal Physical Society*. doi:10.3126/jnphyssoc.v8i2.50148

N, N., P, A., C, L., & D, C. A context-aware machine learning-based approach. *Conference of the Centre for Advanced Studies on Collaborative Researc h*.

Nadkarni, P. M., Ohno-Machado, L., & Chapman, W. W. (2011). Natural language processing: an introduction. *Journal of the American Medical Informatics Association, 18*(5), 544-551.

Nagakura, K. <b>Recent Studies on Wayside Environmental Problems</b&gt. *Quarterly Report of RTRI, 58*(2), 88-92. doi:10.2219/rtriqr.58.2_88

Nahar, J., Imam, T., Tickle, K. S., & Chen, Y.-P. P. (2013). Computational intelligence for heart disease diagnosis: A medical knowledge driven approach. *Expert Systems with Applications, 40*(1), 96-104.

Nair, V., & Hinton, G. E. (2010). *Rectified linear units improve restricted boltzmann machines.* Paper presented at the Icml.

Nalchigar, S., Yu, E., Obeidi, Y., Carbajales, S., Green, J., & Chan, A. (2019). Solution Patterns for Machine Learning. In *Lecture Notes in Computer Science* (pp. 627-642): Springer International Publishing.

Nan, W., Stanislaw, J., Kyunghyun, C., & Krzysztof, J. G. Characterizing and overcoming the greedy nature of learning in multi-m odal deep neural networks. *International Conference on Machine Learning*.

Nan, Z., Zhu, G., Zhang, X., Lin, X., & Yang, Y. A Novel High-Precision Railway Obstacle Detection Algorithm Based on 3 D LiDAR. *Sensors, 24*(10), 3148. doi:10.3390/s24103148

Napierala, K., & Stefanowski, J. Types of minority class examples and their influence on learning class ifiers from imbalanced data. *Journal of Intelligent Information Systems, 46*(3), 563-597. doi:10.1007/s10844-015-0368-1

Nargesian, F., Samulowitz, H., Khurana, U., Khalil, E. B., & Turaga, D. (2017/8//). *Learning Feature Engineering for Classification*.

Narwane, S. V., & Sawarkar, S. D. Is handling unbalanced datasets for machine learning uplifts system pe rformance?: A case of diabetic prediction. *Diabetes & Metabolic Syndrome: Clinical Research & Reviews, 16*(9), 102609. doi:10.1016/j.dsx.2022.102609

Naseriparsa, M., Al-Shammari, A., Sheng, M., Zhang, Y., & Zhou, R. (2020). RSMOTE: improving classification performance over imbalanced medical datasets. *Health information science and systems, 8*, 1-13.

Nasri, M., Kargahi, M., & Mohaqeqi, M. Scheduling of Accuracy-Constrained Real-Time Systems in Dynamic Enviro nments. *IEEE Embedded Systems Letters, 4*(3), 61-64. doi:10.1109/les.2012.2195294

Natrayan, L., Kamal, M. D. R., Manivannan, K. K., & Sunil, G. (2024/1/27/). *Machine Learning and Data Mining Approaches for Infectious Disease Sur veillance and Outbreak Management in Healthcare*.

Nay, J., & Strandburg, K. J. (2021). Generalizability: machine learning and humans-in-the-loop. In *Research handbook on big data law* (pp. 285-303): Edward Elgar Publishing.

Nayak, D., & Tantravahi, S. L. R. On building machine learning models for medical dataset with correlate d features. *Computational and Mathematical Biophysics, 12*(1). doi:10.1515/cmb-2023-0124

Nedungadi, P., & Smruthy, T. K. (2015). Personalized Multi-relational Matrix Factorization Model for Predictin g Student Performance. In *Advances in Intelligent Systems and Computing* (pp. 163-172): Springer International Publishing.

Neil, A. T., & M, J. W. Automated De-Identification: Embracing the Imperfect. *Radiology: Artificial Intelligence*. doi:10.1148/ryai.2020200230

Neil, C. T., K, G., Keeheon, L., & Gabriel, F. M. The Computational Limits of Deep Learning. *Ninth Computing within Limits 2023*. doi:10.21428/bf6fb269.1f033948

Nelson, K., Corbin, G., & Blowers, M. (2014/5/22/). *Evaluating data distribution and drift vulnerabilities of machine lear ning algorithms in secure and adversarial environments*.

Newell, A., & Simon, H. A. (1972). *Human problem solving* (Vol. 104): Prentice-hall Englewood Cliffs, NJ.

Newell, B. R., McDonald, R. I., Brewer, M., & Hayes, B. K. The Psychology of Environmental Decisions. *Annual Review of Environment and Resources, 39*(1), 443-467. doi:10.1146/annurev-environ-010713-094623

Ngiam, J., Peng, D., Vasudevan, V., Kornblith, S., Le, Q. V., & Pang, R. (2018). Domain adaptive transfer learning with specialist models. *arXiv preprint arXiv:1811.07056*.

Nguyen, T., & Pernkopf, F. (2019). *Acoustic Scene Classification with Mismatched Devices Using CliqueNets and Mixup Data Augmentation.* Paper presented at the Interspeech.

Nguyen, V. D., Van Nguyen, H., Tran, D. T., Lee, S. J., & Jeon, J. W. (2016). Learning framework for robust obstacle detection, recognition, and tracking. *IEEE Transactions on Intelligent Transportation Systems, 18*(6), 1633-1646.

Nicholas, G. P., & Vadim, O. S. Deep learning: Computational aspects. *WIREs Computational Statistics*. doi:10.1002/wics.1500

Nicolas, P. Security and Privacy in Machine Learning.

Nicolas, P., P, M., Arunesh, S., & Michael, P. W. Towards the Science of Security and Privacy in Machine Learning. *arXiv.org*.

Nijgal, D. R., George, S., & Subramanian, P. (2023/7/6/). *Evaluating the Effectiveness of a Facial Recognition-Based Attendance Management System in a Real-World Setting*.

Nikolikj, A., Kostovska, A., Cenikj, G., Doerr, C., & Eftimov, T. (2024/6/30/).

*Generalization Ability of Feature-Based Performance Prediction Models: A Statistical Analysis Across Benchmarks*.

Nishihara, R., Moritz, P., Wang, S., Tumanov, A., Paul, W., Schleier-Smith, J., . . . Stoica, I. (2017/5/7/). *Real-Time Machine Learning*.

Nordhaus, W. D. (2001). The progress of computing. *Available at SSRN 285168*.

O, A., & R, D. The Promise of Machine Learning: When Will it be Delivered? *Journal of Cardiac Failure*. doi:10.1016/j.cardfail.2019.04.006

Obaid, L., Hamad, K., Khalil, M. A., & Nassif, A. B. Effect of feature optimization on performance of machine learning mode ls for predicting traffic incident duration. *Engineering Applications of Artificial Intelligence, 131*, 107845. doi:10.1016/j.engappai.2024.107845

Ognjen, R., Jaeryoung, L., Miles, D., Björn, S., & Rosalind, W. P. Personalized machine learning for robot perception of affect and engag ement in autism therapy. *Science Robotics*. doi:10.1126/scirobotics.aao6760

Ogunleye, A., & Wang, Q.-G. (2019). XGBoost model for chronic kidney disease diagnosis. *IEEE/ACM transactions on computational biology and bioinformatics, 17*(6), 2131-2140.

Ojha, V. K., Griego, D., Kuliga, S., Bielik, M., Buš, P., Schaeben, C., . . . Schmitt, G. Machine learning approaches to understand the influence of urban envir onments on human's physiological response. *Information Sciences, 474*, 154-169. doi:10.1016/j.ins.2018.09.061

Ojtáš, P., & Peška, L. (2014). *e-Shop User Preferences via User Behavior*.

Oliphant, T. E. (2006a). Guide to numpy. In: Trelgol Publishing USA.

Oliphant, T. E. (2006b). *A guide to NumPy* (Vol. 1): Trelgol Publishing USA.

Omar, Y. A.-J., Paul, Y., S, M., G, K., & K, T. Efficient Machine Learning for Big Data: A Review. *Big Data Research*. doi:10.1016/j.bdr.2015.04.001

Organization, W. H. (2017). *Global hepatitis report 2017*: World Health Organization.

Organization, W. H. (2022). Invisible numbers: the true extent of noncommunicable diseases and what to do about them.

Orji, F. A., & Vassileva, J. Machine Learning Approach for Predicting Students Academic Performance and Study Strategies based on their Motivation. *arXiv.org*. doi:10.48550/ARXIV.2210.08186

Ornish, D., Brown, S. E., Billings, J., Scherwitz, L., Armstrong, W. T., Ports, T. A., . . . Brand, R. (1990). Can lifestyle changes reverse coronary heart disease?: The Lifestyle Heart Trial. *The Lancet, 336*(8708), 129-133.

Ortega, F., Bobadilla, J., Hernando, A., & Gutiérrez, A. Incorporating group recommendations to recommender systems: Alternativ es and performance. *Information Processing & Management, 49*(4), 895-901. doi:10.1016/j.ipm.2013.02.003

Oussama, E. G., S, H., Yasser, L., Mohamed, A. M., B, C., & A, R. Improving skin diseases prediction through data balancing via classes weighting and transfer learning. *Bulletin of Electrical Engineering and Informatics*. doi:10.11591/eei.v13i1.5999

P, G., Petko, V., & R, S. Impact of Biases in Big Data. *The European Symposium on Artificial Neural Networks*.

P. Bharathi, D., Ravindra, P., & R. Kiran, K. Machine learning solutions for the healthcare industry: A review. *i-manager's Journal on Artificial Intelligence & Machine Learning, 1*(1), 41. doi:10.26634/jaim.1.1.19230

Pablo, B. o., Mikaël, M., Jorge, A. P. e., & Bernardo, S. Model Interpretability through the Lens of Computational Complexity. *Neural Information Processing Systems*.

Padilla, R., Netto, S. L., & Da Silva, E. A. (2020). *A survey on performance metrics for object-detection algorithms.* Paper presented at the 2020 international conference on systems, signals and image processing (IWSSIP).

Paleyes, A., Urma, R.-G., & Lawrence, N. D. Challenges in Deploying Machine Learning: A Survey of Case Studies. *ACM Computing Surveys, 55*(6), 1-29. doi:10.1145/3533378

Pan, B., Panda, R., Jiang, Y., Wang, Z., Feris, R., & Oliva, A. (2021). IA-RED $^ 2$: Interpretability-Aware Redundancy Reduction for Vision Transformers. *Advances in Neural Information Processing Systems, 34*, 24898-24911.

Pan, I., Mason, L. R., & Matar, O. K. Data-centric Engineering: integrating simulation, machine learning and statistics. Challenges and opportunities. *Chemical Engineering Science, 249*, 117271. doi:10.1016/j.ces.2021.117271

Pant, A. Importance of Data Security and Privacy Compliance. *International Journal for Research in Applied Science and Engineering Technology, 11*(11), 1561-1565. doi:10.22214/ijraset.2023.56862

Papernot, N., McDaniel, P., Sinha, A., & Wellman, M. P. (2018/4//). *SoK: Security and Privacy in Machine Learning*.

Paraskevi, C., & Konstantinos, L. Data Protection Issues in Automated Decision-Making Systems Based on M achine Learning: Research Challenges. *Network*. doi:10.3390/network4010005

Park, K. H., Chung, H., & Kwon, S. Towards an Efficient ML System: Unveiling a Trade-off between Task Acc uracy and Engineering Efficiency in a Large-scale Car Sharing Platform. *arXiv.org*. doi:10.48550/ARXIV.2210.06585

Park, S. (2021). *Bridging Multi-disciplinary Collaboration Challenges in ML Development via Domain Knowledge Elicitation*.

Park, Y. S., Konge, L., & Artino, A. R. (2020). The positivism paradigm of research. *Academic Medicine, 95*(5), 690-694.

Parks, L., & Guay, R. P. Can Personal Values Predict Performance? Evidence in an Academic Setti ng. *Applied Psychology, 61*(1), 149-173. doi:10.1111/j.1464-0597.2011.00461.x

Paszke, A., Gross, S., Massa, F., Lerer, A., Bradbury, J., Chanan, G., . . . Antiga, L. (2019). Pytorch: An imperative style, high-performance deep learning library. *Advances in neural information processing systems, 32*.

Pattanayak, S. S., & Rout, M. (2017). Experimental Comparison of Sampling Techniques for Imbalanced Datasets Using Various Classification Models. In *Advances in Intelligent Systems and Computing* (pp. 13-22): Springer Singapore.

Patton, M. Q. (2014). *Qualitative research & evaluation methods: Integrating theory and practice*: Sage publications.

Paul, A. K., Shill, P. C., Rabin, M. R. I., & Akhand, M. (2016). *Genetic algorithm based fuzzy decision support system for the diagnosis of heart disease.* Paper presented at the 2016 5th International Conference on Informatics, Electronics and Vision (ICIEV).

Paul, A. K., Shill, P. C., Rabin, M. R. I., & Murase, K. (2018). Adaptive weighted fuzzy rule-based system for the risk level assessment of heart disease. *Applied Intelligence, 48*, 1739-1756.

Pawlotsky, J.-M., Bouvier-Alias, M., Hezode, C., Darthuy, F., Remire, J., &

Dhumeaux, D. (2000). Standardization of hepatitis C virus RNA quantification. *Hepatology, 32*(3), 654-659.

Pearl, J. (2018/2/2/). *Theoretical Impediments to Machine Learning With Seven Sparks from the Causal Revolution*.

Peiró, J. M., Bayona, J. A., Caballer, A., & Di Fabio, A. Importance of work characteristics affects job performance: The mediat ing role of individual dispositions on the work design-performance rel ationships. *Personality and Individual Differences, 157*, 109808. doi:10.1016/j.paid.2019.109808

Peng, J., Mei, X., Li, W., Hong, L., Sun, B., & Li, H. Scene Complexity: A New Perspective on Understanding the Scene Semanti cs of Remote Sensing and Designing Image-Adaptive Convolutional Neural Networks. *Remote Sensing, 13*(4), 742. doi:10.3390/rs13040742

Peng, S., Niemeyer, M., Mescheder, L., Pollefeys, M., & Geiger, A. (2020). *Convolutional occupancy networks.* Paper presented at the Computer Vision–ECCV 2020: 16th European Conference, Glasgow, UK, August 23–28, 2020, Proceedings, Part III 16.

Pengtao, X. Diversity-Promoting and Large-Scale Machine Learning for Healthcare. *Carnegie Mellon University*. doi:10.1184/R1/7553468.V1

Peter, F. S., & S, S. A Framework for Individualizing Predictions of Disease Trajectories by Exploiting Multi-Resolution Structure. *Neural Information Processing Systems*.

Peters, J. R. (2007). *Machine learning of motor skills for robotics*: University of Southern California.

Peterson, L. E. (2009). K-nearest neighbor. *Scholarpedia, 4*(2), 1883.

Pfeifer, N., & Böhm, J. (2008). *Early stages of LiDAR data processing.* Paper presented at the Li, Z., Chen, J., and Baltsavias, E., Advanced in Photogrammetry, Remote Sensing and Spatial Information Sciences: 2008 ISPRS Congress Book, CRC Press/Balkema, Leiden, The Netherlands.

Pfohl, S. R., Foryciarz, A., & Shah, N. H. An empirical characterization of fair machine learning for clinical ri sk prediction. *Journal of Biomedical Informatics, 113*, 103621. doi:10.1016/j.jbi.2020.103621

Phuong, M., & Lampert, C. (2019). *Towards understanding knowledge distillation.* Paper presented at the International Conference on Machine Learning.

Piratla, V. Robustness, Evaluation and Adaptation of Machine Learning Models in th e Wild. *arXiv.org*. doi:10.48550/ARXIV.2303.02781

Pirk, S., Krs, V., Hu, K., Rajasekaran, S. D., Kang, H., Yoshiyasu, Y., . . . Guibas, L. J. Understanding and Exploiting Object Interaction Landscapes. *ACM Transactions on Graphics, 36*(3), 1-14. doi:10.1145/3083725

Poghosyan, G., Pefkianakis, I., Le Guyadec, P., & Christophides, V. (2017/7//). *Extracting usage patterns of home IoT devices*.

Polat, K. (2018). Similarity-based attribute weighting methods via clustering algorithms in the classification of imbalanced medical datasets. *Neural Computing and Applications, 30*, 987-1013.

Popov, S., Morozov, S., & Babenko, A. (2019). Neural oblivious decision ensembles for deep learning on tabular data. *arXiv preprint arXiv:1909.06312*.

Popper, K. (2005). *The logic of scientific discovery*: Routledge.

Porta, A., Baselli, G., Lombardi, F., Montano, N., Malliani, A., & Cerutti, S. (1999). Conditional entropy approach for the evaluation of the coupling strength. *Biological*

*cybernetics, 81*, 119-129.

Poynard, T., Yuen, M.-F., Ratzin, V., & Lai, C. L. (2003). Viral hepatitis C. *The Lancet, 362*(9401), 2095-2100.

Prabhakar, G., Kailath, B., Natarajan, S., & Kumar, R. (2017). *Obstacle detection and classification using deep learning for tracking in high-speed autonomous driving.* Paper presented at the 2017 IEEE region 10 symposium (TENSYMP).

Pradipta, G. A., Wardoyo, R., Musdholifah, A., Sanjaya, I. N. H., & Ismail, M. (2021). *SMOTE for handling imbalanced data problem: A review.* Paper presented at the 2021 sixth international conference on informatics and computing (ICIC).

Prado, F. F., & Digiampietri, L. A. (2020/11/3/). *A systematic review of automated feature engineering solutions in mach ine learning problems*.

Prateek, G. Integrating Differential Privacy and HE for Enhanced Privacy and Secur ity in FL without Compromising Model Utility. *2023 International Conference on Power Energy, Environment & Intellige nt Control (PEEIC)*. doi:10.1109/PEEIC59336.2023.10451626

Prechelt, L. (1998). Automatic early stopping using cross validation: quantifying the criteria. *Neural Networks, 11*(4), 761-767.

Prechelt, L. (2012). Early stopping—but when? *Neural networks: tricks of the trade: second edition*, 53-67.

Preuveneers, D., Tsingenopoulos, I., & Joosen, W. Resource Usage and Performance Trade-offs for Machine Learning Models in Smart Environments. *Sensors, 20*(4), 1176. doi:10.3390/s20041176

Proceedings of the 2023 6th International Conference on Machine Vision and Applications. *International Conference on Machine Vision and Applications*. doi:10.1145/3589572

Prokhorenkova, L., Gusev, G., Vorobev, A., Dorogush, A. V., & Gulin, A. (2018). CatBoost: unbiased boosting with categorical features. *Advances in Neural Information Processing Systems, 31*.

Provost, F. (2016/2/8/). *The Predictive Power of Massive Data about our Fine-Grained Behavior*.

Purushotham, S., & Jay Kuo, C. C. (2015). Modeling Group Dynamics for Personalized Group-Event Recommendation. In *Lecture Notes in Computer Science* (pp. 405-411): Springer International Publishing.

Putatunda, S., & Rama, K. (2018). *A comparative analysis of hyperopt as against other approaches for hyper-parameter optimization of XGBoost.* Paper presented at the Proceedings of the 2018 international conference on signal processing and machine learning.

Qi, C. R., Su, H., Mo, K., & Guibas, L. J. (2017). *Pointnet: Deep learning on point sets for 3d classification and segmentation.* Paper presented at the Proceedings of the IEEE conference on computer vision and pattern recognition.

Qi, C. R., Yi, L., Su, H., & Guibas, L. J. (2017). Pointnet++: Deep hierarchical feature learning on point sets in a metric space. *Advances in Neural Information Processing Systems, 30*.

Qian, Z., F, M. H., G, A., & J, K. Explicit or implicit feedback? engagement or satisfaction?: a field ex periment on machine-learning-based recommender systems. *ACM Symposium on Applied Computing*. doi:10.1145/3167132.3167275

Qiu, G., Kuang, D., & Goel, S. Complexity Matters: Dynamics of Feature Learning

in the Presence of Sp urious Correlations. *arXiv.org*. doi:10.48550/ARXIV.2403.03375

Qiu, J., Wu, Q., Ding, G., Xu, Y., & Feng, S. (2016). A survey of machine learning for big data processing. *EURASIP Journal on Advances in Signal Processing, 2016*, 1-16.

Quaglietta, E., Corman, F., & Goverde, R. M. P. Stability analysis of railway dispatching plans in a stochastic and dy namic environment. *Journal of Rail Transport Planning & Management, 3*(4), 137-149. doi:10.1016/j.jrtpm.2013.10.009

Quan, H., Sundararajan, V., Halfon, P., Fong, A., Burnand, B., Luthi, J.-C., . . . Ghali, W. A. (2005). Coding algorithms for defining comorbidities in ICD-9-CM and ICD-10 administrative data. *Medical care*, 1130-1139.

Quinlan, J. R. (1986). Induction of decision trees. *Machine learning, 1*(1), 81-106.

Quinlan, J. R. (1987). Simplifying decision trees. *International journal of man-machine studies, 27*(3), 221-234.

R ECOGNIZING AND OVERCOMING THE GREEDY NA - TURE OF LEARNING IN MULTI - MODAL DEEP NEURAL NETWORKS.

R, M. Big Data, Machine Learning, Consumer Protection and Privacy.

R, M., T, P., S, G., & J, B. Exploiting dynamic aspects of visual perception for object recognition. *Proceedings of PerAc '94. From Perception to Action*. doi:10.1109/FPA.1994.636104

R, V. K., A, T., Shravani, N., S, S., & Sankalp, C. Exploring Scalable and Efficient Deployment of Machine Learning Models : A Comparative Analysis of Amazon SageMaker and Heroku. *2023 International Conference on Information Technology (ICIT)*. doi:10.1109/ICIT58056.2023.10225793

Radford, A., Wu, J., Child, R., Luan, D., Amodei, D., & Sutskever, I. (2019). Language models are unsupervised multitask learners. *OpenAI blog, 1*(8), 9.

Raghavendra, S., Julian, S., & Erik, D. Operating critical machine learning models in resource constrained reg imes. *MTSAIL/LEAF/AI4Treat/MMMI/REMIA@MICCAI*. doi:10.1007/978-3-031-47425-5_29

Raihan, M., Mandal, P. K., Islam, M. M., Hossain, T., Ghosh, P., Shaj, S. A., . . . More, A. (2019). *Risk prediction of ischemic heart disease using artificial neural network.* Paper presented at the 2019 international conference on electrical, computer and communication engineering (ECCE).

Raj, T., Hanim Hashim, F., Baseri Huddin, A., Ibrahim, M. F., & Hussain, A. (2020). A survey on LiDAR scanning mechanisms. *Electronics, 9*(5), 741.

Rajan, T. S., Chavan, G. T., Kumar, R., Saini, R., Rajesh, A., & Doda, D. K. (2023/12/29/). *Leveraging Machine Learning for More Efficient Real-Time Data Analysis*.

Rajaraman, S., Zamzmi, G., Yang, F., Xue, Z., & Antani, S. K. (2023). Data Characterization for Reliable AI in Medicine. In *Communications in Computer and Information Science* (pp. 3-11): Springer Nature Switzerland.

Rajput, S. L., Tripathi, A. M., & Maurya, M. Exploring the role of feature engineering in enhancing machine learnin g models for sales prediction in the retail sector. *International Journal of Applied Research, 4*(8), 108-111. doi:10.22271/allresearch.2018.v4.i8b.11447

Ramasubramanian, K., & Singh, A. (2018). Feature Engineering. In *Machine Learning Using R* (pp. 211-251): Apress.

Ravita, C., & Deepinder, K. A systematic review of the machine learning algorithms for the computa tional analysis in different domains. *International Journal of Advanced Technology and Engineering Explorati on*. doi:10.19101/ijatee.2020.762057

Rawat, W., & Wang, Z. (2017). Deep convolutional neural networks for image classification: A comprehensive review. *Neural computation, 29*(9), 2352-2449.

Rawlinson, D., & Kowadlo, G. (2017). Computational Neuroscience Offers Hints for More General Machine Learn ing. In *Lecture Notes in Computer Science* (pp. 123-132): Springer International Publishing.

Razmi, N., & Nassar, M. R. Adaptive learning through temporal dynamics of state representation. *Journal of Neuroscience*. doi:10.1101/2020.08.03.231068

Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). *You only look once: Unified, real-time object detection.* Paper presented at the Proceedings of the IEEE conference on computer vision and pattern recognition.

Reed, R. (1993). Pruning algorithms-a survey. *IEEE transactions on neural networks, 4*(5), 740-747.

Register, L. s. DATA QUALITY CONSIDERATIONS FOR PETROPHYSICAL MACHINE LEARNING MODELS. In: Society of Petrophysicists and Well Log Analysts.

Reitinger, N., Wen, B., Mazurek, M. L., & Ur, B. (2023/11/26/). *Analysis of Google Ads Settings Over Time: Updated, Individualized, Ac curate, and Filtered*.

Rembold, C. M. (1998). Number needed to screen: development of a statistic for disease screening. *Bmj, 317*(7154), 307-312.

Ren, S., He, K., Girshick, R., & Sun, J. (2015). Faster r-cnn: Towards real-time object detection with region proposal networks. *Advances in Neural Information Processing Systems, 28*.

Renyu, Y., Ouyang, X., Yaofeng, C., P, T., & Jie, X. Intelligent Resource Scheduling at Scale: A Machine Learning Perspecti ve. *International Symposium on Service Oriented Software Engineering*. doi:10.1109/SOSE.2018.00025

Rezak, A., S, B., S, B., & Thinh, L. V. Exploring Homomorphic Encryption and Differential Privacy Techniques t owards Secure Federated Learning Paradigm. *Future Internet*. doi:10.3390/fi15090310

Ribeiro, J., & Elsayed, E. (1995). A case study on process optimization using the gradient loss function. *International Journal of Production Research, 33*(12), 3233-3248.

Ribezzi-Crivellari, M., & Ritort, F. (2019). Large work extraction and the Landauer limit in a continuous Maxwell demon. *Nature Physics, 15*(7), 660-664.

Richter, A. N., Khoshgoftaar, T. M., Landset, S., & Hasanin, T. (2015/8//). *A Multi-dimensional Comparison of Toolkits for Machine Learning with B ig Data*.

Rifkin, J. (2011). *The third industrial revolution: how lateral power is transforming energy, the economy, and the world*: Macmillan.

Rifqi, F., & Deni, M. SYSTEMATIC LITERATURE REVIEW OF THE CLASS IMBALANCE CHALLENGES IN MAC HINE LEARNING. *Jurnal Teknik Informatika (Jutif), 4*(5), 1099-1107. doi:10.52436/1.jutif.2023.4.5.970

Ríos-Sánchez, B., Costa-da-Silva, D., Martín-Yuste, N., & Sánchez-Ávila, C. Deep Learning for Facial Recognition on Single Sample per Person Scena rios with Varied Capturing Conditions. *Applied Sciences, 9*(24), 5474. doi:10.3390/app9245474

Ristić-Durrant, D., Haseeb, M. A., Banić, M., Stamenković, D., Simonović, M., & Nikolić, D. SMART on-board multi-sensor obstacle detection system for improvement of rail transport safety. *Proceedings of the Institution of Mechanical Engineers, Part F: Journa l of Rail and Rapid Transit, 236*(6), 623-636. doi:10.1177/09544097211032738

Robert, A., Saketh, R., Brandon, R., Gu-Yeon, W., & D, B. Fathom: reference workloads for modern deep learning methods. *IEEE International Symposium on Workload*

*Characterization*. doi:10.1109/IISWC.2016.7581275

Robert, P., Daniel, T., & Peizhao, H. SoK: Privacy-preserving Deep Learning with Homomorphic Encryption. *arXiv.org*.

Robert, P., Daniel, T., Peizhao, H., M, R., & Zhipeng, C. A Survey of Deep Learning Architectures for Privacy-Preserving Machine Learning With Fully Homomorphic Encryption. *IEEE Access*. doi:10.1109/ACCESS.2022.3219049

Rockwood, K. An Individualized Approach to Tracking and Treating Alzheimer's Diseas e. *Clinical Pharmacology & Therapeutics, 88*(4), 446-449. doi:10.1038/clpt.2010.68

Rodriguez-Andina, J. J., Moure, M. J., & Valdes, M. D. (2007). Features, design tools, and application domains of FPGAs. *IEEE Transactions on Industrial Electronics, 54*(4), 1810-1823.

Romero, A., Ballas, N., Kahou, S. E., Chassang, A., Gatta, C., & Bengio, Y. (2014). Fitnets: Hints for thin deep nets. *arXiv preprint arXiv:1412.6550*.

Roriz, R., Cabral, J., & Gomes, T. (2021). Automotive LiDAR technology: A survey. *IEEE Transactions on Intelligent Transportation Systems, 23*(7), 6282-6297.

Rosenberg, A., & Hirschberg, J. (2007). *V-measure: A conditional entropy-based external cluster evaluation measure.* Paper presented at the Proceedings of the 2007 joint conference on empirical methods in natural language processing and computational natural language learning (EMNLP-CoNLL).

Roth, G. (2018). Global burden of disease collaborative network. global burden of disease study 2017 (GBD 2017) results. Seattle, United States: Institute for health metrics and evaluation (IHME), 2018. *Lancet, 392*, 1736-1788.

Rousson, V., & Gooniu, N. F. (2007). An R-square coefficient based on final prediction error. *Statistical Methodology, 4*(3), 331-340.

Rozianiwati, Y., K, A. K., A, M., N, M., & N, M. Z. Techniques for handling imbalanced datasets when producing classifier models.

Rudin, C. Stop explaining black box machine learning models for high stakes deci sions and use interpretable models instead. *Nature Machine Intelligence, 1*(5), 206-215. doi:10.1038/s42256-019-0048-x

Rudin, C., Chen, C., Chen, Z., Huang, H., Semenova, L., & Zhong, C. (2022). Interpretable machine learning: Fundamental principles and 10 grand challenges. *Statistic Surveys, 16*, 1-85.

Rumelhart, D. E., Hinton, G. E., & McClelland, J. L. (1986). A general framework for parallel distributed processing. *Parallel distributed processing: Explorations in the microstructure of cognition, 1*(45-76), 26.

Rumelhart, D. E., Hinton, G. E., & Williams, R. J. (1986). Learning representations by back-propagating errors. *nature, 323*(6088), 533-536.

Rumelhart, D. E., McClelland, J. L., & Group, P. R. (1988). *Parallel distributed processing* (Vol. 1): IEEE New York.

Runhua, X., N, B., & J, J. Privacy-Preserving Machine Learning: Methods, Challenges and Direction s. *arXiv.org*.

Runnalls, A. R. (2007). Kullback-Leibler approach to Gaussian mixture reduction. *IEEE Transactions on Aerospace and Electronic Systems, 43*(3), 989-999.

Russakovsky, O., Deng, J., Su, H., Krause, J., Satheesh, S., Ma, S., . . . Bernstein, M. (2015). Imagenet large scale visual recognition challenge. *International journal of computer vision, 115*(3), 211-252.

S, A. G., & Mudasir, K. Diversity of Information Sources in the Digital Age: An Overview.

S, B.-D., S, B., Karsten, M. B., Michael, B., David, C., Amir, G., . . . Masashi, S. Machine Learning in Non-Stationary Environments - Introduction to Cova riate Shift Adaptation. *Adaptive computation and machine learning*.

S, G. De-Identification of Personal Information. doi:10.6028/NIST.IR.8053

S, G., Julián, L., & Francisco, H. Dealing with Noisy Data. doi:10.1007/978-3-319-10247-4_5

S, K. M., & R, S. ML Privacy Meter: Aiding Regulatory Compliance by Quantifying the Priv acy Risks of Machine Learning. *arXiv.org*.

S, M., Aitzaz, N., Jeff, D., & Stan, G. Improving the Performance of Fine-Grain Image Classifiers via Generati ve Data Augmentation. *arXiv.org*.

S, M., S, Y., H, G., Stefan, M., & Patrick, M. BEVDetNet: Bird's Eye View LiDAR Point Cloud based Real-time 3D Object Detection for Autonomous Driving. *International Conference on Intelligent Transportation Systems*. doi:10.1109/ITSC48978.2021.9564490

S, T., Alessandro, B., Francesco, F., & G, R. Physical-Layer Location Verification by Machine Learning. doi:10.1002/9781119562306.ch20

Sachchidanand, S., Naveen, S., & V, S. Comparative Analysis of Open Standards for Machine Learning Model Depl oyments. *ICT Systems and Sustainability*. doi:10.1007/978-981-16-5987-4_51

Sagar, S., Deepali, K., & V, K. Informed Active Learning to Aid Domain Experts in Modeling Compliance. *IEEE International Enterprise Distributed Object Computing Conference*. doi:10.1109/EDOC.2016.7579382

Sahoo, K., Samal, A. K., Pramanik, J., & Pani, S. K. (2019). Exploratory data analysis using Python. *International Journal of Innovative Technology and Exploring Engineering, 8*(12), 4727-4735.

Saini, G., Seema, & Mor, K. Machine Learning and Prophecy of Behavior: A Breakthrough in Artificia l Intelligence. *IOP Conference Series: Materials Science and Engineering, 1099*(1), 012026. doi:10.1088/1757-899x/1099/1/012026

Samuel, A., E, F., Orna, R., Marcel, Z., & Parijat, D. Detection of data drift and outliers affecting machine learning model performance over time. *arXiv.org*.

Sánchez-Marqués, R., García, V., & Sánchez, J. S. A data-centric machine learning approach to improve prediction of glio ma grades using low-imbalance TCGA data. *Scientific Reports, 14*(1). doi:10.1038/s41598-024-68291-0

Sánchez, J., & Perronnin, F. (2011). *High-dimensional signature compression for large-scale image classification.* Paper presented at the CVPR 2011.

Sanders, J., & Kandrot, E. (2010). *CUDA by example: an introduction to general-purpose GPU programming*: Addison-Wesley Professional.

Sandler, M., Howard, A., Zhu, M., Zhmoginov, A., & Chen, L.-C. (2018). *Mobilenetv2: Inverted residuals and linear bottlenecks.* Paper presented at the Proceedings of the IEEE conference on computer vision and pattern recognition.

Santra, A., & Bhowmick, S. (2017). Holistic Analysis of Multi-source, Multi-feature Data: Modeling and Co mputation Challenges. In *Lecture Notes in Computer Science* (pp. 59-68): Springer International Publishing.

Sarah, H. K. Doing data science. *Choice Reviews Online, 51*(12), 51-6803-6851-6803. doi:10.5860/choice.51-6803

Sarker, I. H., Colman, A., Han, J., Khan, A. I., Abushark, Y. B., & Salah, K. BehavDT: A Behavioral Decision Tree Learning to Build User-Centric Con text-Aware Predictive Model. *Mobile Networks and Applications, 25*(3), 1151-1161. doi:10.1007/s11036-019-01443-z

Sarker, I. H., Kayes, A. S. M., & Watters, P. Effectiveness analysis of machine learning classification models for p redicting personalized context-aware smartphone usage. *Journal of Big data, 6*(1). doi:10.1186/s40537-019-0219-y

Sarvesh Koli Komal Bhat Prajwal Korade, D. M. A. M. O. K. o. Unlocking Machine Learning Model Decisions: A Comparative Analysis of LIME and SHAP for Enhanced Interpretability. *Journal of Electrical Systems, 20*(2s), 598-613. doi:10.52783/jes.1480

Sasmal, S. Real-time Data Processing with Machine Learning Algorithms. *INTERNATIONAL RESEARCH JOURNAL OF ENGINEERING & APPLIED SCIENCES, 11*(4), 91-96. doi:10.55083/irjeas.2023.v11i04012

Schaller, R. R. (1997). Moore's law: past, present and future. *IEEE spectrum, 34*(6), 52-59.

Scheuer, P. J., Ashrafzadeh, P., Sherlock, S., Brown, D., & Dusheiko, G. M. (1992). The pathology of hepatitis C. *Hepatology, 15*(4), 567-571.

Schmitt, M. (1989). Mathematical morphology and artificial intelligence: an automatic programming system. *Signal Processing, 16*(4), 389-401.

Schnabel, R., Wahl, R., & Klein, R. (2007). *Efficient RANSAC for point-cloud shape detection.* Paper presented at the Computer graphics forum.

Schramm, P. The Individual True and Error Model: Getting the Most out of Limited D ata. *Judgment and Decision Making*. doi:10.31234/osf.io/p3m4v

Schubert, E., Sander, J., Ester, M., Kriegel, H. P., & Xu, X. (2017). DBSCAN revisited, revisited: why and how you should (still) use DBSCAN. *ACM Transactions on Database Systems (TODS), 42*(3), 1-21.

Schuh, G., Scholz, P., Leich, T., & May, R. (2020/10/15/). *Identifying and Analyzing Data Model Requirements and Technology Poten tials of Machine Learning Systems in the Manufacturing Industry of the Future*.

Schultheis, E., & Babbar, R. (2022). 6.3 Extreme Multicore Classification. *Also of interest*, 272.

Scott, M. L., & Su-In, L. A Unified Approach to Interpreting Model Predictions. *Neural Information Processing Systems*.

Seedat, N., Crabbé, J., Bica, I., & van der Schaar, M. Data-IQ: Characterizing subgroups with heterogeneous outcomes in tabul ar data. *Neural Information Processing Systems*. doi:10.48550/ARXIV.2210.13043

Seeff, L. B. (2002). Natural history of chronic hepatitis C. *Hepatology, 36*(5B), s35-s46.

Sener, O., & Koltun, V. (2018). Multi-task learning as multi-objective optimization. *Advances in Neural Information Processing Systems, 31*.

Seonyeong, H., Sungjun, C., Youngsok, K., & Hanjun, K. Real-Time Object Detection System with Multi-Path Neural Networks. *IEEE Real Time Technology and Applications Symposium*. doi:10.1109/RTAS48715.2020.000-8

Sepas-Moghaddam, A., Malhadas, L., Correia, P. L., & Pereira, F. Face spoofing detection using a light field imaging framework. *IET Biometrics, 7*(1), 39-48. doi:10.1049/iet-bmt.2017.0095

Sethi, T., Kalia, A., Sharma, A., & Nagori, A. (2020). Interpretable artificial

intelligence: Closing the adoption gap in hea lthcare. In *Artificial Intelligence in Precision Health* (pp. 3-29): Elsevier.

Setsobhonkul, S., Kaewunruen, S., & Sussman, J. M. Lifecycle Assessments of Railway Bridge Transitions Exposed to Extreme Climate Events. *Frontiers in Built Environment, 3*. doi:10.3389/fbuil.2017.00035

Sevilla, J., Heim, L., Ho, A., Besiroglu, T., Hobbhahn, M., & Villalobos, P. (2022). Compute trends across three eras of machine learning. *arXiv preprint arXiv:2202.05924*.

Shah, D., Patel, S., & Bharti, S. K. (2020). Heart disease prediction using machine learning techniques. *SN Computer Science, 1*, 1-6.

Shah, R. V., Grennan, G., Zafar-Khan, M., Alim, F., Dey, S., Ramanathan, D., & Mishra, J. Personalized machine learning of depressed mood using wearables. *Translational Psychiatry, 11*(1). doi:10.1038/s41398-021-01445-0

Shahid, I., Alzahrani, A. R., Al-Ghamdi, S. S., Alanazi, I. M., Rehman, S., & Hassan, S. Hepatitis C Diagnosis: Simplified Solutions, Predictive Barriers, and Future Promises. *Diagnostics, 11*(7), 1253. doi:10.3390/diagnostics11071253

Shaikhah, A., & Julita, V. Personalized Recommendation of Research Papers by Fusing Recommendatio ns from Explicit and Implicit Social Network. *User Modeling, Adaptation, and Personalization*.

Shakira, K., V, S., Gnanaprakasam, C. N., T, L., N, D., & N, A. O. Privacy Protection of Healthcare Data over Social Networks Using Machi ne Learning Algorithms. *Computational intelligence and neuroscience*. doi:10.1155/2022/9985933

Shan, Y., Hoens, T. R., Jiao, J., Wang, H., Yu, D., & Mao, J. C. (2016/8/13/). *Deep Crossing*.

Shapere, D. (1964). The structure of scientific revolutions. *The Philosophical Review, 73*(3), 383-394.

Shapiro, L. G., & Stockman, G. C. (2001). *Computer vision* (Vol. 3): Prentice hall New Jersey.

Sharad, G., & D, G. Predicting Individual Behavior with Social Networks. *Marketing science (Providence, R.I.)*. doi:10.1287/mksc.2013.0817

Sharif, M. S., Afolabi, M. O., Zorto, A., & Elmedany, W. (2022/11/20/). *Enhancement Techniques for Improving Facial Recognition Performance in Convolutional Neural Networks*.

Sharma, A., & Dey, S. (2012). *A comparative study of feature selection and machine learning techniques for sentiment analysis.* Paper presented at the Proceedings of the 2012 ACM research in applied computation symposium.

Sharma, N., Chawla, V., & Ram, N. (2020). Comparison of machine learning algorithms for the automatic programming of computer numerical control machine. *International Journal of Data and Network Science, 4*(1), 1-14.

Sharma, R., & Rani, S. Quantified Self: From Self-Learning to Machine Learning. *IT Professional, 23*(4), 69-74. doi:10.1109/mitp.2021.3059485

Shea–Budgell, M. A., Kostaras, X., Myhill, K. P., & Hagen, N. A. Information Needs and Sources of Information for Patients during Cance r Follow-Up. *Current Oncology, 21*(4), 165-173. doi:10.3747/co.21.1932

Shen, X., & Stamos, I. (2020). *Frustum VoxNet for 3D object detection from RGB-D or Depth images.* Paper presented at the Proceedings of the IEEE/CVF winter conference on applications of computer vision.

Shenge, J. A., & Osiowy, C. Rapid Diagnostics for Hepatitis B and C Viruses in Low-

and Middle-Inc ome Countries. *Frontiers in Virology, 1*. doi:10.3389/fviro.2021.742722

Shi-Chieh, L., Yunqi, Z., Chang-Hong, H., Matt, S., Md, E. H., Lingjia, T., & Jason, M. The Architectural Implications of Autonomous Driving: Constraints and Acceleration. *International Conference on Architectural Support for Programming Lang uages and Operating Systems*. doi:10.1145/3173162.3173191

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE internet of things journal, 3*(5), 637-646.

Shihan, W., S, S., Karlijn, S., M, D., J, T., & B, K. What Are Good Situations for Running? A Machine Learning Study Using M obile and Geographical Data. *Frontiers in Public Health*. doi:10.3389/fpubh.2020.536370

Shivakumar, S. S., Nguyen, T., Miller, I. D., Chen, S. W., Kumar, V., & Taylor, C. J. (2019). *Dfusenet: Deep fusion of rgb and sparse depth information for image guided dense depth completion.* Paper presented at the 2019 IEEE Intelligent Transportation Systems Conference (ITSC).

Shixuan, C., Yuchen, G., Yizhou, H., Lilai, S., Qiming, Z., Yaru, P., & Shulin, Z. Advances and applications of machine learning and deep learning in env ironmental ecology and health. *Environmental Pollution*. doi:10.1016/j.envpol.2023.122358

Shodamola, J., Qureshi, H., Masood, U., & Imran, A. (2021/12//). *Towards Addressing the Spatial Sparsity of MDT Reports to Enable Zero Touch Network Automation*.

Shorten, C., & Khoshgoftaar, T. M. A survey on Image Data Augmentation for Deep Learning. *Journal of Big data, 6*(1). doi:10.1186/s40537-019-0197-0

Shorten, C., & Khoshgoftaar, T. M. (2019). A survey on image data augmentation for deep learning. *Journal of Big data, 6*(1), 1-48.

Shukla, A., Pokhariya, H. S., Michaelson, J., Srivastava, A. P., Narayanamma, L., & Srivastava, A. (2023/12/29/). *Enhancing Security and Privacy in Cloud – Based Healthcare Data Throug h Machine Learning*.

Shwartz-Ziv, R., & Armon, A. (2022). Tabular data: Deep learning is not all you need. *Information Fusion, 81*, 84-90.

Siddhant, M. J., Jacob, M., Wojciech, M. C., Jonathan, S., Jack, W. R., Simon, O., . . . Razvan, P. Multiplicative Interactions and Where to Find Them. *International Conference on Learning Representations*.

Siegler, M., Pellegrino, E. D., & Singer, P. A. (1990). Clinical medical ethics. *The Journal of clinical ethics, 1*(1), 5-9.

Silva, P., Silva, C. T., & Nonato, L. G. Exploring the Relationship Between Feature Attribution Methods and Mod el Performance. *arXiv.org*. doi:10.48550/ARXIV.2405.13957

Simonović, M., Banić, M., Stamenković, D., Franke, M., Michels, K., Schoolmann, I., . . . Dimec, M. Toward the Enhancement of Rail Sustainability: Demonstration of a Holi stic Approach to Obstacle Detection in Operational Railway Environment s. *Sustainability, 16*(7), 2613. doi:10.3390/su16072613

Simonyan, K., & Zisserman, A. (2014). Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556*.

Singh, D. K., B, U., Junnarkar, A. A., Singh, V., Singh, M., & R, S. (2023/12/29/). *Harnessing Machine Learning for Increased Efficiency in Real-Time Data Analysis*.

Singh, K., Shah, N. H., & Vickers, A. J. (2023). Assessing the net benefit of machine learning models in the presence of resource constraints. *Journal of the American Medical Informatics Association, 30*(4), 668-673.

Singh, K. D., Saini, G. L., & Singh, P. D. (2023/11/23/). *Leveraging Transfer Learning for Improved Diagnostics in Dermatology*.

Singla, A., K, D., K, M., Kantak, G. K., Singh, A. P., & Rajesh, A. (2023/12/29/). *Improving Real-Time Data Analysis Accuracy with Machine Learning Tools*.

Siriram, R. IMPROVING FORECASTS FOR BETTER DECISION-MAKING. *The South African Journal of Industrial Engineering, 27*(1). doi:10.7166/27-1-486

Smajić, A., Grandits, M., & Ecker, G. F. Privacy-preserving techniques for decentralized and secure machine lea rning in drug discovery. *Drug Discovery Today, 28*(12), 103820. doi:10.1016/j.drudis.2023.103820

Smith, J. E. (1988). Characterizing computer performance with a single number. *Communications of the ACM, 31*(10), 1202-1206.

Somepalli, G., Goldblum, M., Schwarzschild, A., Bruss, C. B., & Goldstein, T. (2021). Saint: Improved neural networks for tabular data via row attention and contrastive pre-training. *arXiv preprint arXiv:2106.01342*.

Song, L., Wang, C., Zhang, L., Du, B., Zhang, Q., Huang, C., & Wang, X. (2020). Unsupervised domain adaptive re-identification: Theory and practice. *Pattern Recognition, 102*, 107173.

Song, R., Wetherall, J., Maskell, S., & Ralph, J. (2020). *Weather Effects on Obstacle Detection for Autonomous Car*.

Song, W., Shi, C., Xiao, Z., Duan, Z., Xu, Y., Zhang, M., & Tang, J. (2019/11/3/). *AutoInt*.

Songzi, L., & Yuan, L. Assessing Social Determinants-Related Performance Bias of Machine Lear ning Models: A case of Hyperchloremia Prediction in ICU Population. *arXiv.org*.

Soroush, B., & Cong, L. NeuOS: A Latency-Predictable Multi-Dimensional Optimization Framework for DNN-driven Autonomous Systems. *USENIX Annual Technical Conference*.

Soule, A., Salamatian, K., & Taft, N. (2005). *Combining filtering and statistical methods for anomaly detection*.

Soumia, Z. E. M., Gabriele, L., & Hüseyin, D. Preserving data privacy in machine learning systems. *Computers & security*. doi:10.1016/j.cose.2023.103605

Soviany, S., & Soviany, C. (2020). Feature Engineering. In *Transactions on Computational Science and Computational Intelligence* (pp. 79-103): Springer International Publishing.

Stachl, C., Au, Q., Schoedel, R., Buschek, D., Völkel, S., Schuwerk, T., . . . Bühner, M. Behavioral Patterns in Smartphone Usage Predict Big Five Personality T raits. doi:10.31234/osf.io/ks4vd

Stetter, C., Menning, P., Sauer, J., Stetter, C., Menning, P., & Sauer, J. Going Beyond Average – Using Machine Learning to Evaluate the Effectiv eness of Environmental Subsidies at Micro-Level. *Unknown*. doi:10.22004/AG.ECON.303699

Steven, P., & T, G. How to Exploit Scene Constraints to Improve Object Categorization Algo rithms for Industrial Applications? *International Conference on Computer Vision Theory and Applications*. doi:10.5220/0004342108270830

Strader, D. B., Wright, T., Thomas, D. L., & Seeff, L. B. (2004). Diagnosis, management, and treatment of hepatitis C. *Hepatology, 39*(4), 1147-1171.

Streit, M., Schulz, H., Lex, A., Schmalstieg, D., & Schumann, H. Model-Driven Design for the Visual Analysis of Heterogeneous Data. *IEEE Transactions on Visualization*

*and Computer Graphics, 18*(6), 998-1010. doi:10.1109/tvcg.2011.108

Stumpf, S., Rajaram, V., Li, L., Burnett, M., Dietterich, T., Sullivan, E., . . . Herlocker, J. (2007/1/28/). *Toward harnessing user feedback for machine learning*.

Subanya, B., & Rajalaxmi, R. (2014). *Feature selection using artificial bee colony for cardiovascular disease classification.* Paper presented at the 2014 International conference on electronics and communication systems (ICECS).

Subasri, V., Krishnan, A., Dhalla, A., Pandya, D., Malkin, D., Razak, F., . . . Dolatabadi, E. Diagnosing and remediating harmful data shifts for the responsible dep loyment of clinical AI models. *medRxiv*. doi:10.1101/2023.03.26.23286718

Sudershan, B., Anurag, M., Prahaladha, M., & Yuvraj, A. MLIoT: An End-to-End Machine Learning System for the Internet-of-Thing s. *International Conference on Internet-of-Things Design and Implementati on*. doi:10.1145/3450268.3453522

Sugiyama, M., & Kawanabe, M. Machine Learning in Non-Stationary Environments. *Adaptive computation and machine learning*. doi:10.7551/mitpress/9780262017091.001.0001

Súkeník, P., & Lampert, C. H. (2022). Generalization in multi-objective machine learning. *arXiv preprint arXiv:2208.13499*.

Sultana, F., Sufian, A., & Dutta, P. (2020). A review of object detection models based on convolutional neural network. *Intelligent computing: image processing based applications*, 1-16.

Sumaiya, P. K. Enhancing User Experience using Machine Learning. *International Journal of Engineering Research and, V7*(02). doi:10.17577/ijertv7is020132

Sun, L. (2020). *Application and improvement of xgboost algorithm based on multiple parameter optimization strategy.* Paper presented at the 2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE).

Sun, L., Yan, Z., Zaganidis, A., Zhao, C., & Duckett, T. (2018). Recurrent-octomap: Learning state-based map refinement for long-term semantic mapping with 3-d-lidar data. *IEEE Robotics and Automation Letters, 3*(4), 3749-3756.

Sun, P., Kretzschmar, H., Dotiwalla, X., Chouard, A., Patnaik, V., Tsui, P., . . . Caine, B. (2020). *Scalability in perception for autonomous driving: Waymo open dataset.* Paper presented at the Proceedings of the IEEE/CVF conference on computer vision and pattern recognition.

Sunil, K. M., Sudarshan, S., & Vipul, T. The impact of imbalanced datasets on machine learning models for rare disease detection: A theoretical exploration. *International Journal of Applied Research*. doi:10.22271/allresearch.2018.v4.i8c.11446

Sunil, Y., Raja, A., & Gurpreet, S. Spatial-temporal models in machine learning: A theoretical exploration of applications. *International Journal of Applied Research*. doi:10.22271/allresearch.2018.v4.i7e.11450

Susan, S., & Tuteja, M. Feature Engineering Versus Deep Learning for Scene Recognition: A Brie f Survey. *International Journal of Image and Graphics*. doi:10.1142/s0219467825500548

Sutter, T., Roth, J. A., Chin-Cheong, K., Hug, B. L., & Vogt, J. E. A comparison of general and disease-specific machine learning models f or the prediction of unplanned hospital readmissions. *Journal of the American Medical Informatics Association, 28*(4), 868-873. doi:10.1093/jamia/ocaa299

Sutton, R. S., & Barto, A. G. (2018). *Reinforcement learning: An introduction*: MIT press.

Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., . . . Rabinovich, A. (2015). *Going deeper with convolutions.* Paper presented at the Proceedings of the IEEE conference on computer vision and pattern recognition.

T, R. H., R, P., & N, C. Learning from streaming data with concept drift and imbalance: an over view. *Progress in Artificial Intelligence*. doi:10.1007/s13748-011-0008-0

Taghikhah, F., Filatova, T., & Voinov, A. Where Does Theory Have It Right? A Comparison of Theory-Driven and Emp irical Agent Based Models. *Journal of Artificial Societies and Social Simulation, 24*(2). doi:10.18564/jasss.4573

Tajbakhsh, N., Shin, J. Y., Gurudu, S. R., Hurst, R. T., Kendall, C. B., Gotway, M. B., & Liang, J. (2016). Convolutional neural networks for medical image analysis: Full training or fine tuning? *IEEE transactions on medical imaging, 35*(5), 1299-1312.

Takale, D. G., Wattamwar, A. A., Saipatwar, S. S., Saindane, H. V., & Patil, T. B. Comparative Analysis of LSTM, RNN, CNN and MLP Machine Learning Algori thms for Stock Value Prediction. *Journal of Firewall Software and Networking, 2*(1), 1-10. doi:10.48001/jofsn.2024.211-10

Tan, C., Sun, F., Kong, T., Zhang, W., Yang, C., & Liu, C. (2018a). *A survey on deep transfer learning.* Paper presented at the Artificial Neural Networks and Machine Learning–ICANN 2018: 27th International Conference on Artificial Neural Networks, Rhodes, Greece, October 4-7, 2018, Proceedings, Part III 27.

Tan, C., Sun, F., Kong, T., Zhang, W., Yang, C., & Liu, C. (2018b). *A survey on deep transfer learning.* Paper presented at the International conference on artificial neural networks.

Tan, M., Chen, B., Pang, R., Vasudevan, V., Sandler, M., Howard, A., & Le, Q. V. (2019). *Mnasnet: Platform-aware neural architecture search for mobile.* Paper presented at the Proceedings of the IEEE/CVF conference on computer vision and pattern recognition.

Tang, W., Chen, W., Amini, A., Boeras, D., Falconer, J., Kelly, H., . . . Easterbrook, P. (2017). Diagnostic accuracy of tests to detect Hepatitis C antibody: a meta-analysis and review of the literature. *BMC infectious diseases, 17*, 39-57.

Tanner, M. A., & Wong, W. H. (1987). The calculation of posterior distributions by data augmentation. *Journal of the American statistical Association, 82*(398), 528-540.

Tanuwidjaja, H. C., Choi, R., & Kim, K. (2019). A Survey on Deep Learning Techniques for Privacy-Preserving. In *Lecture Notes in Computer Science* (pp. 29-46): Springer International Publishing.

Taye, G. D., & Yehualashet, M. A. Deep Learning Models for Audio Processing Applications Under Resource- Constrained Devices: A Survey. *PanAfriCon AI*. doi:10.1007/978-3-031-31327-1_12

Taylor, L., & Nitschke, G. (2018). *Improving deep learning with generic data augmentation.* Paper presented at the 2018 IEEE symposium series on computational intelligence (SSCI).

Taylor, S., Jaques, N., Nosakhare, E., Sano, A., & Picard, R. Personalized Multitask Learning for Predicting Tomorrow's Mood, Stress , and Health. *IEEE Transactions on Affective Computing, 11*(2), 200-213. doi:10.1109/taffc.2017.2784832

Teichman, A., & Thrun, S. (2011/10//). *Practical object recognition in autonomous driving and beyond*.

Tennenholtz, G., Merlis, N., Shani, L., Mladenov, M., & Boutilier, C. Reinforcement Learning with History-Dependent Dynamic Contexts. *International Conference on Machine Learning*. doi:10.48550/ARXIV.2302.02061

Terven, J., & Cordova-Esparza, D. (2023). A comprehensive review of YOLO: From

YOLOv1 to YOLOv8 and beyond. *arXiv preprint arXiv:2304.00501*.

Thabtah, F., Hammoud, S., Kamalov, F., & Gonsalves, A. Data imbalance in classification: Experimental evaluation. *Information Sciences, 513*, 429-441. doi:10.1016/j.ins.2019.11.004

Thapa, B., & Walia, A. (2007). Liver function tests and their interpretation. *The Indian Journal of Pediatrics, 74*, 663-671.

Theis, T. N., & Wong, H.-S. P. (2017). The end of moore's law: A new beginning for information technology. *Computing in Science & Engineering, 19*(2), 41-50.

Theodoros, R., X, D., L, G., & D, S. Finding Quality in Quantity: The Challenge of Discovering Valuable Sou rces for Integration. *Conference on Innovative Data Systems Research*.

Thumpati, A., & Zhang, Y. (2023/10/28/). *Towards Optimizing Performance of Machine Learning Algorithms on Unbal anced Dataset*.

Tian, F., Li, H., Chen, W., Qin, T., Chen, E., & Liu, T.-Y. Agent Behavior Prediction and Its Generalization Analysis. *Proceedings of the AAAI Conference on Artificial Intelligence, 28*(1). doi:10.1609/aaai.v28i1.8914

Tian, J., Jin, Q., Wang, Y., Yang, J., Zhang, S., & Sun, D. Performance analysis of deep learning-based object detection algorithm s on COCO benchmark: a comparative study. *Journal of Engineering and Applied Science, 71*(1). doi:10.1186/s44147-024-00411-z

Tian, Y., Yang, G., Wang, Z., Wang, H., Li, E., & Liang, Z. (2019). Apple detection during different growth stages in orchards using the improved YOLO-V3 model. *Computers and electronics in agriculture, 157*, 417-426.

Tianci, Z., Jinglong, C., Fudong, L., Kaiyu, Z., Haixin, L., Shuilong, H., & Enyong, X. Intelligent fault diagnosis of machines with small & imbalanced data: A state-of-the-art review and possible extensions. *ISA transactions*. doi:10.1016/j.isatra.2021.02.042

Tianxi, L., E, L., & Ji, Z. Prediction models for network-linked data. *Annals of Applied Statistics*. doi:10.1214/18-AOAS1205

Tim, R., S, M., Julian, P., & Bernd, Z. Using Domain-Knowledge to Improve Machine Learning. *atp magazin*. doi:10.17560/atp.v63i9.2600

Time Series Data Preparation. *Machine Learning for Time Series Forecasting with Python®*, 61-99. doi:10.1002/9781119682394.ch3

Timothée, L., Massimo, C., & I, R. Understanding Continual Learning Settings with Data Distribution Drift Analysis. *arXiv.org*.

Timothy, D., Katherine, K., Michael, M., & Luca, V. Why Providing Humans with Interpretable Algorithms May, Counterintuiti vely, Lead to Lower Decision-making Performance. *Social Science Research Network*. doi:10.2139/ssrn.4246077

Ting, Y. Incorporating prior domain knowledge into inductive machine learning : its implementation in contemporary capital markets.

Ting, Y., S, S., & T, J. VQSVM: A case study for incorporating prior domain knowledge into indu ctive machine learning. *Neurocomputing*. doi:10.1016/j.neucom.2010.05.007

Tiwari, R. K., Dubey, S. K., & Kumar, V. Interpretability machine learning models: A critical analysis of techn iques and applications. *The Pharma Innovation, 8*(2S), 25-28. doi:10.22271/tpi.2019.v8.i2sa.25245

Tobias, B., & M, V. Parallel Retrieval of Dense Vectors in the Vector Space Model. *Computing and informatics*.

Tobin, P., & Blackledge, J. (2014). *Entropy, information, Landauer's limit and Moore's law.* Paper presented at the 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014).

Torlay, L., Perrone-Bertolotti, M., Thomas, E., & Baciu, M. (2017). Machine learning–XGBoost analysis of language networks to classify patients with epilepsy. *Brain informatics, 4*, 159-169.

Torrey, L., & Shavlik, J. (2010). Transfer learning. In *Handbook of research on machine learning applications and trends: algorithms, methods, and techniques* (pp. 242-264): IGI global.

Tosi, S. (2009). *Matplotlib for Python developers*: Packt Publishing Ltd.

Tu, W., Zhou, S., Liu, X., Guo, X., Cai, Z., Zhu, E., & Cheng, J. (2021). *Deep fusion clustering network.* Paper presented at the Proceedings of the AAAI Conference on Artificial Intelligence.

Tyagi, S., & Mittal, S. (2019). Sampling Approaches for Imbalanced Data Classification Problem in Mach ine Learning. In *Lecture Notes in Electrical Engineering* (pp. 209-221): Springer International Publishing.

Tzu-Hsien, Y., Zhan-Yi, L., Yu-Huai, Y., & Min, H. RDDL: A systematic ensemble pipeline tool that streamlines balancing t raining schemes to reduce the effects of data imbalance in rare-diseas e-related deep-learning applications. *Comput. Biol. Chem.* doi:10.1016/j.compbiolchem.2023.107929

Tzvika, H., M, H., J, D., S, H., Ronit, S., Itay, L., . . . Yossi, M. Customization scenarios for de-identification of clinical notes. *BMC Medical Informatics and Decision Making*. doi:10.1186/s12911-020-1026-2

Uddin, V., Rizvi, S. S. H., Hashmani, M. A., Jameel, S. M., & Ansari, T. (2019). A Study of Deterioration in Classification Models in Real-Time Big Dat a Environment. In *Advances in Intelligent Systems and Computing* (pp. 79-87): Springer International Publishing.

Uher, R. Genes, Environment, and Individual Differences in Responding to Treatm ent for Depression. *Harvard Review of Psychiatry, 19*(3), 109-124. doi:10.3109/10673229.2011.586551

Ul Ghani, M. A. N., She, K., Saeed, M. U., & Latif, N. Enhancing facial recognition accuracy through multi-scale feature fusi on and spatial attention mechanisms. *Electronic Research Archive, 32*(4), 2267-2285. doi:10.3934/era.2024103

Ulf, B. Interdisciplinary Machine Learning. *LWA*.

Ullah, I., R, M., & Shihao, Y. Machine Learning and Location Verification in Vehicular Networks. *International Conference on Innovative Computing and Cloud Computing*. doi:10.1109/ICCChina.2019.8855920

United Nations Industrial Development Organization, U. N. I. D. Q. (2021). *International Yearbook of Industrial Statistics 2021* (Vol. 880): Edward Elgar.

Upadhyay, U., Kumar, A., Roy, S., & Rawat, U. Balancing innovation and privacy : A machine learning perspective. *Journal of Discrete Mathematical Sciences and Cryptography, 27*(2-B), 547-557. doi:10.47974/jdmsc-1877

Vaeyens, R., Lenoir, M., Williams, A. M., Mazyn, L., & Philippaerts, R. M. The Effects of Task Constraints on Visual Search Behavior and Decision -Making Skill in Youth Soccer Players. *Journal of Sport and Exercise Psychology, 29*(2), 147-169. doi:10.1123/jsep.29.2.147

Vaid, A., Sawant, A., Suarez-Farinas, M., Lee, J., Kaul, S., Kovatch, P., . . . Nadkarni,

G. N. Real-world usage diminishes validity of Artificial Intelligence tools. *medRxiv*. doi:10.1101/2022.11.17.22282440

Valentina, Z., A, B., & M, T. Fully Decentralized Joint Learning of Personalized Models and Collabor ation Graphs. *International Conference on Artificial Intelligence and Statistics*.

Van Der Bom, T., Zomer, A. C., Zwinderman, A. H., Meijboom, F. J., Bouma, B. J., & Mulder, B. J. (2011). The changing epidemiology of congenital heart disease. *Nature Reviews Cardiology, 8*(1), 50-60.

Van Dyk, D. A., & Meng, X.-L. (2001). The art of data augmentation. *Journal of Computational and Graphical Statistics, 10*(1), 1-50.

Van Erven, T., & Harremos, P. (2014). Rényi divergence and Kullback-Leibler divergence. *IEEE Transactions on Information Theory, 60*(7), 3797-3820.

van Giffen, B., Herhausen, D., & Fahse, T. Overcoming the pitfalls and perils of algorithms: A classification of machine learning biases and mitigation methods. *Journal of Business Research, 144*, 93-106. doi:10.1016/j.jbusres.2022.01.076

Van Houdt, G., Mosquera, C., & Nápoles, G. (2020). A review on the long short-term memory model. *Artificial Intelligence Review, 53*, 5929-5955.

Vanholder, H. (2016). *Efficient inference with tensorrt.* Paper presented at the GPU Technology Conference.

Vapnik, V. (1998). The support vector method of function estimation. In *Nonlinear modeling* (pp. 55-85): Springer.

Vapnik, V. (1999a). *The nature of statistical learning theory*: Springer science & business media.

Vapnik, V. (1999b). An overview of statistical learning theory. *IEEE transactions on neural networks, 10*(5), 988-999.

Varsha, B. Classification of Imbalanced Data of Medical Diagnosis using Sampling Techniques. doi:10.5120/CAE2021652883

Varun, O. Do the dynamics of the city environment influence us, and how? Answer through the Machine Learning Approaches.

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., . . . Polosukhin, I. (2017a). Attention is all you need. *Advances in neural information processing systems, 30*.

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., . . . Polosukhin, I. (2017b). *Attention is all you need.* Paper presented at the Advances in neural information processing systems.

Veatch, R. M. (1997). *Medical ethics*: Jones & Bartlett Learning.

Velliangiri, S., Alagumuthukrishnan, S., & Thankumar joseph, S. I. A Review of Dimensionality Reduction Techniques for Efficient Computat ion. *Procedia Computer Science, 165*, 104-111. doi:10.1016/j.procs.2020.01.079

Venkateswara, S. B., & Suman, D. A Risk Based Approach for Privacy Compliant Machine Learning Lifecycle. *2022 2nd International Conference on Intelligent Technologies (CONIT)*. doi:10.1109/CONIT55038.2022.9847739

Vera, A. H., & Simon, H. A. (1993). Situated action: A symbolic interpretation. *Cognitive science, 17*(1), 7-48.

Verdonck, T., Baesens, B., Óskarsdóttir, M., & vanden Broucke, S. (2021). Special issue on feature engineering editorial. *Machine learning*, 1-12.

Verdú, S. (1990). On channel capacity per unit cost. *IEEE Transactions on Information Theory, 36*(5), 1019-1030.

Verdú, S. (1994). A general formula for channel capacity. *IEEE Transactions on Information Theory, 40*(4), 1147-1157.

Vickerman, R. (1997). High-speed rail in Europe: experience and issues for future development. *The annals of regional science, 31*, 21-38.

Vij, P., & Dalip, D. (2023/7/6/). *Performance Analysis of Dimensionality Reduction Techniques for Datase ts using Deep Learning*.

Villar, L. M., Cruz, H. M., Barbosa, J. R., Bezerra, C. S., Portilho, M. M., & Scalioni, L. d. P. Update on hepatitis B and C virus diagnosis. *World Journal of Virology, 4*(4), 323. doi:10.5501/wjv.v4.i4.323

Villareale, J., Harteveld, C., & Zhu, J. "I Want To See How Smart This AI Really Is": Player Mental Model Devel opment of an Adversarial AI Player. *Proceedings of the ACM on Human-Computer Interaction, 6*(CHI PLAY), 1-26. doi:10.1145/3549482

Vipin, G., Shailendra, S., & Kumari, N. Cracking the Code: Enhancing Trust in AI through Explainable Models. *resmilitaris, 10*(1). doi:10.48047/resmil.v10i1.20

Virani, N., Ji-Woong, L., Phoha, S., & Ray, A. (2015/7//). *Learning context-aware measurement models*.

Vishnuvardhan, G., & Ravi, V. (2021). Face Recognition Using Transfer Learning on Facenet: Application to Ba nking Operations. In *Studies in Computational Intelligence* (pp. 301-309): Springer International Publishing.

Vitor, R., Eduardo, H. M. P., Raphael, S., Reza, A., P, V., Falaah, A. K., . . . Fábio, P. Subset Modelling: A Domain Partitioning Strategy for Data-efficient Ma chine-Learning. *Brazilian Symposium on Databases*. doi:10.5753/sbbd.2023.232829

Vogelsang, A., & Borg, M. (2019/9//). *Requirements Engineering for Machine Learning: Perspectives from Data Scientists*.

Voulodimos, A., Doulamis, N., Doulamis, A., & Protopapadakis, E. (2018). Deep learning for computer vision: A brief review. *Computational intelligence and neuroscience, 2018*.

W, S., G, M., Alexander, B., Sebastian, L., & K, M. Interpreting the Predictions of Complex ML Models by Layer-wise Releva nce Propagation. *arXiv.org*.

Wandinger, U. (2005). Introduction to lidar. In *Lidar: range-resolved optical remote sensing of the atmosphere* (pp. 1-18): Springer.

Wang, A., Pruksachatkun, Y., Nangia, N., Singh, A., Michael, J., Hill, F., . . . Bowman, S. (2019). Superglue: A stickier benchmark for general-purpose language understanding systems. *Advances in neural information processing systems, 32*.

Wang, B. A Parallel Implementation of Computing Mean Average Precision. *arXiv.org*. doi:10.48550/ARXIV.2206.09504

Wang, C., Li, M., & Smola, A. J. (2019). Language models with transformers. *arXiv preprint arXiv:1904.09408*.

Wang, D., Gong, C., & Liu, Q. (2019). *Improving neural language modeling via adversarial training.* Paper presented at the International Conference on Machine Learning.

Wang, D., Zhang, Y., & Zhao, Y. (2017). *LightGBM: an effective miRNA classification method in breast cancer patients.* Paper presented at the Proceedings of the 2017 international conference on computational biology and bioinformatics.

Wang, H., Lei, Z., Zhang, X., Zhou, B., & Peng, J. (2016). Machine learning basics.

*Deep learning*, 98-164.

Wang, J., Lan, C., Liu, C., Ouyang, Y., Zeng, W., & Qin, T. (2021). Generalizing to unseen domains: A survey on domain generalization. *arXiv preprint arXiv:2103.03097*.

Wang, J., & Perez, L. (2017). The effectiveness of data augmentation in image classification using deep learning. *Convolutional Neural Networks Vis. Recognit, 11*(2017), 1-8.

Wang, Q., Ma, Y., Zhao, K., & Tian, Y. (2020). A comprehensive survey of loss functions in machine learning. *Annals of Data Science*, 1-26.

Wang, R., Chaudhari, P., & Davatzikos, C. Bias in machine learning models can be significantly mitigated by care ful training: Evidence from neuroimaging studies. *Proceedings of the National Academy of Sciences, 120*(6). doi:10.1073/pnas.2211613120

Wang, R., Shen, Y., Tino, P., Welchman, A. E., & Kourtzi, Z. Learning predictive statistics from temporal sequences: Dynamics and s trategies. *Journal of Vision, 17*(12), 1. doi:10.1167/17.12.1

Wang, X. (2022/7/1/). *A framework for Requirements specification of machine-learning systems*.

Wang, X., Qu, C., Wu, W., Wang, J., & Zhou, Q. Are we ready for learned cardinality estimation? *Proceedings of the VLDB Endowment, 14*(9), 1640-1654. doi:10.14778/3461535.3461552

Wang, Z., Wohlwend, J., & Lei, T. (2019). Structured pruning of large language models. *arXiv preprint arXiv:1910.04732*.

Waqar, M., Dawood, H., Dawood, H., Majeed, N., Banjar, A., & Alharbey, R. (2021). An efficient SMOTE-based deep learning model for heart attack prediction. *Scientific Programming, 2021*, 1-12.

Waskom, M. (2021). seaborn: Statistical data visualization: Journal of Open Source Software, v. 6. In.

Watthaisong, T., Sunat, K., & Muangkote, N. Comparative Evaluation of Imbalanced Data Management Techniques for So lving Classification Problems on Imbalanced Datasets. *Statistics, Optimization & Information Computing, 12*(2), 547-570. doi:10.19139/soic-2310-5070-1890

Wei, H., Zhengdong, Z., Benjamin, C., Brandon, Y., Christoph, S., O, A., . . . Z, C. Streaming Object Detection for 3-D Point Clouds. *European Conference on Computer Vision*. doi:10.1007/978-3-030-58523-5_25

Wei, W., Shibo, Z., Jingxi, L., Xiaohua, L., Junsong, Y., & Zhanpeng, J. Temporal Pulses Driven Spiking Neural Network for Fast Object Recognit ion in Autonomous Driving. *arXiv.org*.

Weichselbaum, J., Zinner, C., Gebauer, O., & Pree, W. (2013). Accurate 3D-vision-based obstacle detection for an autonomous train. *Computers in Industry, 64*(9), 1209-1220.

Weiss, K., Khoshgoftaar, T. M., & Wang, D. (2016). A survey of transfer learning. *Journal of Big data, 3*, 1-40.

Weiss, K., Khoshgoftaar, T. M., & Wang, D. (2016). A survey of transfer learning. *Journal of Big Data, 3*(1), 1-40.

Weixian, L., Rong, Z., Yang, Y., Ruixuan, W., & Weishi, Z. Class-Center Involved Triplet Loss for Skin Disease Classification on Imbalanced Data. *IEEE International Symposium on Biomedical Imaging*. doi:10.1109/ISBI45749.2020.9098718

Wen, Q., Yang, L., Zhou, T., & Sun, L. (2022/8/14/). *Robust Time Series Analysis and Applications*.

Wen, W., Xu, C., Wu, C., Wang, Y., Chen, Y., & Li, H. (2017). *Coordinating filters for faster deep neural networks.* Paper presented at the Proceedings of the IEEE International Conference on Computer Vision.

Westermann, H., Šavelka, J., Walker, V. R., Ashley, K. D., & Benyekhlef, K. (2021). Data-Centric Machine Learning: Improving Model Performance and Underst anding Through Dataset Analysis. In *Frontiers in Artificial Intelligence and Applications*: IOS Press.

Wibowo, P., & Fatichah, C. An in-depth performance analysis of the oversampling techniques for hi gh-class imbalanced dataset. *Register: Jurnal Ilmiah Teknologi Sistem Informasi, 7*(1), 63. doi:10.26594/register.v7i1.2206

Wiharto, W., Kusnanto, H., & Herianto, H. (2016). Intelligence system for diagnosis level of coronary heart disease with K-star algorithm. *Healthcare informatics research, 22*(1), 30-38.

Wijeyakulasuriya, D. A., Eisenhauer, E. W., Shaby, B. A., & Hanks, E. M. Machine learning for modeling animal movement. *PLoS ONE, 15*(7), e0235750. doi:10.1371/journal.pone.0235750

Wiley, V., & Lucas, T. (2018). Computer vision and image processing: a paper review. *International Journal of Artificial Intelligence Research, 2*(1), 29-36.

Wilson, J. M. G., Jungner, G., & Organization, W. H. (1968). Principles and practice of screening for disease.

Winograd, S. (1980). *Arithmetic complexity of computations* (Vol. 33): Siam.

Wirges, S., Fischer, T., Stiller, C., & Frias, J. B. (2018). *Object detection and classification in occupancy grid maps using deep convolutional networks.* Paper presented at the 2018 21st International Conference on Intelligent Transportation Systems (ITSC).

Wójtowicz, A., & Chmielewski, J. (2020). Analysis of Factors Improving Accuracy of Passive User Identification with Streams of Face Images for Ubiquitous Commerce. In *Lecture Notes in Computer Science* (pp. 271-284): Springer International Publishing.

Won-Seok, J., Hansaem, J., Kyungtae, K., N, D., & Jong-Chan, K. R-TOD: Real-Time Object Detector with Minimized End-to-End Delay for A utonomous Driving. *IEEE Real-Time Systems Symposium*. doi:10.1109/RTSS49844.2020.00027

Wong, S. C., Gatt, A., Stamatescu, V., & McDonnell, M. D. (2016). *Understanding data augmentation for classification: when to warp?* Paper presented at the 2016 international conference on digital image computing: techniques and applications (DICTA).

Wong, T.-T., & Yeh, P.-Y. (2019). Reliable accuracy estimates from k-fold cross validation. *IEEE Transactions on Knowledge and Data Engineering, 32*(8), 1586-1594.

Wonsuk, K., & Junhee, S. Privacy-preserving collaborative machine learning in biomedical applic ations. *Digital Signal Processing and Signal Processing Education Workshop*. doi:10.1109/ICAIIC54071.2022.9722703

World Health Organization, D. (2020). Global health estimates 2020: deaths by cause, age, sex, by country and by region, 2000-2019. In: Who Geneva, Switzerland.

Wörmann, J., Bogdoll, D., Brunner, C., Bührle, E., Chen, H., Chuo, E. F., . . . Zwicklbauer, S. Knowledge Augmented Machine Learning with Applications in Autonomous D riving: A Survey. *arXiv.org*. doi:10.48550/ARXIV.2205.04712

Wright, A. G. C., & Woods, W. C. Personalized Models of Psychopathology. *Annual Review of Clinical Psychology*. doi:10.31234/osf.io/6hqzj

Wu, K., Wu, E., & Kreiman, G. (2018/3//). *Learning scene gist with convolutional neural networks to improve obje ct recognition*.

Wu, X., Sahoo, D., & Hoi, S. C. (2020). Recent advances in deep learning for object detection. *Neurocomputing, 396*, 39-64.

Wu, Y., Wang, Y., Zhang, S., & Ogai, H. (2020). Deep 3D object detection networks using LiDAR data: A review. *IEEE Sensors Journal, 21*(2), 1152-1171.

Xi-Zhu, W., & Zhi-Hua, Z. Model reuse with domain knowledge. doi:10.1360/N112017-00106

Xiao, J., Ye, H., He, X., Zhang, H., Wu, F., & Chua, T.-S. (2017/8//). *Attentional Factorization Machines: Learning the Weight of Feature Int eractions via Attention Networks*.

Xin, G., Fariza, S., Zongwen, F., & S, S. A Review of Privacy Enhancement Methods for Federated Learning in Heal thcare Systems. *International Journal of Environmental Research and Public Health*. doi:10.3390/ijerph20156539

Xu, M., David, J. M., & Kim, S. H. (2018). The fourth industrial revolution: Opportunities and challenges. *International journal of financial research, 9*(2), 90-95.

Xu, X., Dong, S., Xu, T., Ding, L., Wang, J., Jiang, P., . . . Li, J. (2023). Fusionrcnn: Lidar-camera fusion for two-stage 3d object detection. *Remote Sensing, 15*(7), 1839.

Yadav, S., & Shukla, S. (2016). *Analysis of k-fold cross-validation over hold-out validation on colossal datasets for quality classification.* Paper presented at the 2016 IEEE 6th International conference on advanced computing (IACC).

Yaghtin, S., & Mero, J. Augmenting machine learning with human insights: the model development for B2B personalization. *Journal of Business & Industrial Marketing, 39*(6), 1192-1208. doi:10.1108/jbim-02-2023-0073

Yan, D., Wang, W., & Chu, X. (2020). *Optimizing batched winograd convolution on GPUs.* Paper presented at the Proceedings of the 25th ACM SIGPLAN symposium on principles and practice of parallel programming.

Yang, H. S., Pan, W., Wang, Y., Zaydman, M. A., Spies, N. C., Zhao, Z., . . . Wang, F. Generalizability of a Machine Learning Model for Improving Utilization of Parathyroid Hormone-Related Peptide Testing across Multiple Clinic al Centers. *Clinical Chemistry, 69*(11), 1260-1269. doi:10.1093/clinchem/hvad141

Yang, H. S., Rhoads, D. D., Sepulveda, J., Zang, C., Chadburn, A., & Wang, F. Building the Model. *Archives of Pathology & Laboratory Medicine, 147*(7), 826-836. doi:10.5858/arpa.2021-0635-ra

Yang, Y., & Nenkova, A. Detecting Information-Dense Texts in Multiple News Domains. *Proceedings of the AAAI Conference on Artificial Intelligence, 28*(1). doi:10.1609/aaai.v28i1.8943

Yao, H. Towards Reliable Learning in the Wild: Generalization and Adaptation. *Proceedings of the AAAI Conference on Artificial Intelligence, 38*(20), 22683-22683. doi:10.1609/aaai.v38i20.30299

Yao, H. (2024). *Towards Reliable Learning in the Wild: Generalization and Adaptation.* Paper presented at the Proceedings of the AAAI Conference on Artificial Intelligence.

Yao, H., Choi, C., Cao, B., Lee, Y., Koh, P. W., & Finn, C. Wild-Time: A Benchmark of in-the-Wild Distribution Shift over Time. *Neural Information Processing Systems*. doi:10.48550/ARXIV.2211.14238

Yasuhiro, W., H, W., Kazunori, S., Daisuke, S., Kiyoshi, H., Naohiko, T., . . . Nobukazu, Y. Preliminary Systematic Literature Review of Machine Learning System De velopment Process. *arXiv.org*.

Yaswanthram, P., & Sabarish, B. A. (2022/1/10/). *Face Recognition Using Machine Learning Models - Comparative Analysis and impact of dimensionality reduction*.

Ye, S., Natarajan, M., Wu, Z., Paleja, R., Chen, L., & Gombolay, M. C. (2023/10/1/). *Learning Models of Adversarial Agent Behavior Under Partial Observabil ity*.

Yim, J., Joo, D., Bae, J., & Kim, J. (2017). *A gift from knowledge distillation: Fast optimization, network minimization and transfer learning.* Paper presented at the Proceedings of the IEEE conference on computer vision and pattern recognition.

Yin, J., Tang, T., Yang, L., Xun, J., Huang, Y., & Gao, Z. (2017). Research and development of automatic train operation for railway transportation systems: A survey. *Transportation Research Part C: Emerging Technologies, 85*, 548-572.

Yin, Z., Sulieman, L. M., & Malin, B. A. A systematic literature review of machine learning in online personal health data. *Journal of the American Medical Informatics Association, 26*(6), 561-576. doi:10.1093/jamia/ocz009

Yiyi, L., Kodagoda, S., Yue, W., Lei, S., & Yong, L. (2016/5//). *Understand scene categories by objects: A semantic regularized scene c lassifier using Convolutional Neural Networks*.

Yongxiang, G., Qianlei, W., & Xiaolin, Q. Real-time Streaming Perception System for Autonomous Driving. *ACM Cloud and Autonomic Computing Conference*. doi:10.1109/CAC53003.2021.9728221

Yoon, C. H., Torrance, R., & Scheinerman, N. Machine learning in medicine: should the pursuit of enhanced interpret ability be abandoned? *Journal of Medical Ethics, 48*(9), 581-585. doi:10.1136/medethics-2020-107102

Yoshua, B., & Yann, L. Scaling learning algorithms towards AI.

Yu, H., Chenzhuang, D., Zihui, X., Xuanyao, C., Hang, Z., & Longbo, H. What Makes Multimodal Learning Better than Single (Provably). *Neural Information Processing Systems*.

Yu, H., Klerman, E. B., Picard, R. W., & Sano, A. (2019/5//). *Personalized Wellbeing Prediction using Behavioral, Physiological and Weather Data*.

Yu, M., Yang, P., & Wei, S. (2018). *Railway obstacle detection algorithm using neural network.* Paper presented at the AIP Conference Proceedings.

Yu, X., & Marinov, M. A Study on Recent Developments and Issues with Obstacle Detection Syst ems for Automated Vehicles. *Sustainability, 12*(8), 3281. doi:10.3390/su12083281

Zamanakos, G., Tsochatzidis, L., Amanatiadis, A., & Pratikakis, I. (2021). A comprehensive survey of LIDAR-based 3D object detection methods with deep learning for autonomous driving. *Computers & Graphics, 99*, 153-181.

Zamani, H., & Bendersky, M. (2023/7/18/). *Multivariate Representation Learning for Information Retrieval*.

Zeiler, M. D., & Fergus, R. (2013). Stochastic pooling for regularization of deep convolutional neural networks. *arXiv preprint arXiv:1301.3557*.

Zejnilovic, L., Lavado, S., Soares, C., Martínez De Rituerto De Troya, Í., Bell, A., & Ghani, R. Machine Learning Informed Decision-Making with Interpreted Model's Out puts: A Field Intervention. *Academy of Management Proceedings, 2021*(1), 15424. doi:10.5465/ambpp.2021.264

Zeng, W., & Chen, L. (2013). Recommending Interest Groups to Social Media Users by Incorporating He terogeneous Resources. In *Lecture Notes in Computer Science* (pp. 361-371): Springer Berlin Heidelberg.

Zezhen, H., & Yaron, S. Visualizing The Implicit Model Selection Tradeoff. *Journal of artificial intelligence research*. doi:10.2139/ssrn.3946701

Zhang, C. State-of-the-Art Approaches to Enhancing Privacy Preservation of Machi ne Learning Datasets: A Survey. *arXiv.org*. doi:10.48550/ARXIV.2404.16847

Zhang, D., Yang, J., Ye, D., & Hua, G. (2018). *Lq-nets: Learned quantization for highly accurate and compact deep neural networks.* Paper presented at the Proceedings of the European conference on computer vision (ECCV).

Zhang, H., Cisse, M., Dauphin, Y. N., & Lopez-Paz, D. (2017). mixup: Beyond empirical risk minimization. *arXiv preprint arXiv:1710.09412*.

Zhang, L., Fu, S., Jiang, S., Bao, R., & Zeng, Y. (2018). A Fusion Model of Multi-data Sources for User Profiling in Social Medi a. In *Lecture Notes in Computer Science* (pp. 3-15): Springer International Publishing.

Zhang, L., Wei, L., Shen, P., Wei, W., Zhu, G., & Song, J. (2018). Semantic SLAM based on object detection and improved octomap. *IEEE Access, 6*, 75545-75559.

Zhang, W., Valencia, A., & Chang, N.-B. Synergistic Integration Between Machine Learning and Agent-Based Model ing: A Multidisciplinary Review. *IEEE Transactions on Neural Networks and Learning Systems, 34*(5), 2170-2190. doi:10.1109/tnnls.2021.3106777

Zhang, W., Zhao, X., Morvan, J.-M., & Chen, L. Improving Shadow Suppression for Illumination Robust Face Recognition. *IEEE transactions on pattern analysis and machine intelligence, 41*(3), 611-624. doi:10.1109/tpami.2018.2803179

Zhang, X., Zhou, X., Lin, M., & Sun, J. (2018). *Shufflenet: An extremely efficient convolutional neural network for mobile devices.* Paper presented at the Proceedings of the IEEE conference on computer vision and pattern recognition.

Zhao, H., Dan, C., Aragam, B., Jaakkola, T. S., Gordon, G. J., & Ravikumar, P. (2022). Fundamental limits and tradeoffs in invariant representation learning. *Journal of machine learning research, 23*(340), 1-49.

Zhao, T., McAuley, J., & King, I. (2014/11/3/). *Leveraging Social Connections to Improve Personalized Ranking for Coll aborative Filtering*.

Zhao, Y., Chetty, G., & Tran, D. (2019). *Deep learning with XGBoost for real estate appraisal.* Paper presented at the 2019 IEEE symposium series on computational intelligence (SSCI).

Zhao, Z.-Q., Zheng, P., Xu, S.-t., & Wu, X. (2019). Object detection with deep learning: A review. *IEEE Transactions on Neural Networks and Learning Systems, 30*(11), 3212-3232.

Zhe, Z., Bingzhe, W., Zheng, L., Guangyu, S., Chenren, X., & Guojie, L. SaFace: Towards Scenario-aware Face Recognition via Edge Computing Sys tem. *USENIX Workshop on Hot Topics in Edge Computing*.

Zheng, A., & Casari, A. (2018). *Feature engineering for machine learning: principles and techniques for data scientists*: " O'Reilly Media, Inc.".

Zheng, H., Hu, H., & Han, Z. Preserving User Privacy for Machine Learning: Local Differential Priva cy or Federated Machine Learning? *IEEE Intelligent Systems, 35*(4), 5-14. doi:10.1109/mis.2020.3010335

Zhenge, J., Jianxu, C., Xiaowei, X., J, K., Jingtong, H., Han, X., . . . Yi, S. The importance of resource awareness in artificial intelligence for he althcare. *Nature Machine Intelligence*. doi:10.1038/s42256-023-00670-0

Zhiyuan, C., & B, L. Topic Modeling using Topics from Many Domains, Lifelong

Learning and B ig Data. *International Conference on Machine Learning*.

Zhong, H., Wang, H., Wu, Z., Zhang, C., Zheng, Y., & Tang, T. (2021). A survey of LiDAR and camera fusion enhancement. *Procedia Computer Science, 183*, 579-588.

Zhou, J., Arshad, S. Z., Yu, K., & Chen, F. (2016). *Correlation for user confidence in predictive decision making*.

Zhou, K., Liu, Z., Qiao, Y., Xiang, T., & Change Loy, C. (2021). Domain generalization: A survey. *arXiv e-prints*, arXiv: 2103.02503.

Zhou, L., & Shen, Z. (2011). Progress in high-speed train technology around the world. *Journal of Modern Transportation, 19*, 1-6.

Zhou, Q.-Y., Park, J., & Koltun, V. (2018). Open3D: A modern library for 3D data processing. *arXiv preprint arXiv:1801.09847*.

Zhou, Z.-H. (2021). *Machine learning*: Springer nature.

Zhouyuan, C., Zhichao, L., & Zhe, X. Interpretable Model-Agnostic Explanations Based on Feature Relationshi ps for High-Performance Computing. *Axioms*. doi:10.3390/axioms12100997

Zhu, C., Han, S., Mao, H., & Dally, W. J. (2016). Trained ternary quantization. *arXiv preprint arXiv:1612.01064*.

Zhu, X., & Goldberg, A. B. (2009). Introduction to semi-supervised learning. *Synthesis lectures on artificial intelligence and machine learning, 3*(1), 1-130.

Zhu, X. J. (2005). Semi-supervised learning literature survey.

Zhu, Y., Wang, W., Lewis, R., Yan, W., Lewis, S. R., & Ding, H. A Review on Wear Between Railway Wheels and Rails Under Environmental Conditions. *Journal of Tribology, 141*(12). doi:10.1115/1.4044464

Zhuang, F., Qi, Z., Duan, K., Xi, D., Zhu, Y., Zhu, H., . . . He, Q. (2020). A comprehensive survey on transfer learning. *Proceedings of the IEEE, 109*(1), 43-76.

Ziang, X., Sarah, M., Bernd, H., Adam, S., & Jennifer, T.-S. Let Me Ask You This: How Can a Voice Assistant Elicit Explicit User Fe edback? *Proc. ACM Hum. Comput. Interact.* doi:10.1145/3479532

Zilong, Z., R, B., Rui, H., B, R., S, B., Sonia, B. M., & L, C. Enhancing Robustness of On-Line Learning Models on Highly Noisy Data. *IEEE Transactions on Dependable and Secure Computing*. doi:10.1109/TDSC.2021.3063947

Zoph, B., & Le, Q. V. (2016). Neural architecture search with reinforcement learning. *arXiv preprint arXiv:1611.01578*.

Zuckerman, I., Kraus, S., Rosenschein, J. S., & Kaminka, G. (2007/5/14/). *An adversarial environment model for bounded rational agents in zero-s um interactions*.