Enhancing Cyber Threat Detection on the Internet of Healthcare Thing Devices Using Hybrid CNN-Federated Learning Algorithms

by Agbessi Kotoklo

B.S. in Mathematics & Economics, December 2009, University of Maryland College Park, Maryland
M.S. in Cybersecurity, August 2012, University of Maryland, University College, College Park, Maryland

A Praxis submitted to

The Faculty of
The School of Engineering and Applied Science
of The George Washington University
in partial fulfillment of the requirements
for the degree of Doctor of Engineering

August 31, 2024

Praxis directed by

Hamza F. Alsarhan
Professorial Lecturer of Engineering Management and Systems Engineering

The School of Engineering and Applied Science of The George Washington University certifies that Agbessi Kotoklo has passed the Final Examination for the degree of Doctor of Engineering as of July 22, 2024. This is the final and approved form of the Praxis.

Enhancing Cyber Threat Detection on the Internet of Healthcare Thing Devices Using Hybrid CNN-Federated Learning Algorithms

Agbessi Kotoklo

Praxis Research Committee:

Dr. Hamza F. Alsarhan, Professorial Lecturer in Engineering and Applied Science, Praxis Director

Dr. Amir Etemadi, Associate Professor of Online Engineering Programs, Committee Chair

Dr. Andrea Molina, Professorial Lecturer in Engineering and Applied Science, Committee Member

© Copyright 2024 by Agbessi Kotoklo
All rights reserved

Dedication

First and foremost, I would like to thank God for his unwavering presence in my life and for being my source of strength and resilience, which enabled me to pursue and achieve this doctorate degree.

Secondly, I would like to dedicate this praxis to my beloved wife, Sayi, and two children, Ethan, and Nathan. Their unwavering love and sacrifices have been the cornerstone of my academic journey, providing the motivation and support I needed to complete this program.

Finally, I would also like to acknowledge my friends and extended family for their steadfast support, encouragement, and understanding throughout my journey in the doctoral program. Their love and support have been a constant source of strength and motivation.

Acknowledgements

I want to express my heartfelt gratitude to Dr. Hamza F Alsarhan and the praxis research committee for their unwavering support and guidance in completing this research. Their collective wisdom and encouragement have been a great learning experience for me, and this research project would not have been successful without their input and cooperation.

Abstract of Praxis

Enhancing Cyber Threat Detection on the Internet of Healthcare Thing Devices Using Hybrid CNN-Federated Learning Algorithms

The introduction of the Internet of Things (IoT) technology into how daily routines has sparked a technological revolution across all sectors of society. The inclusion of these IoT technologies in the healthcare sector eventually resulted in the emergence of a new subdomain of the IoT called the Internet of Healthcare Things (IoHT) technologies, which collect and transmit health-related information to healthcare providers in near-real time. While IoHT has the potential to offer benefits by bringing better care and streamlining data management, it can also create new cybersecurity challenges as well as privacy issues.

This praxis examines the critical issue of IoHT cybersecurity and privacy. It focuses on building a robust privacy-preserving Intrusion Detection System (IDS) by integrating properties of Convolutional Neural Networks (CNNs) and Federated Learning (FL). In general, most solutions for cyber threat detection in the IoT world, such as signature-based and anomaly detection techniques, cannot deal by themselves with the sophistication and dynamics of modern cyber threats. There is a need for a more sophisticated and adaptive approach solution to ensure that critical IoHT components are secure. Furthermore, specifically in healthcare, it is not just about data integrity of data but also about keeping patient safe and their valuable health information confidential.

This praxis aims to improve the security and privacy of IoHT devices by developing a hybrid deep learning model that includes the federated learning method.

Federated learning is a machine learning approach that operates in a decentralizing manner by allowing multiple devices to collaborate in training a global model while retaining the data on each device at a localized level. This is generally a robust technique that could be potentially suitable for healthcare environments, where data privacy and security are of utmost importance. This is because it reduces the chance of vital data leakage and fulfills rigid healthcare regulations.

The binary and multi-class classification tasks have been tested for the CNN-FL model using the ECU-IoHT dataset. Various metrics for evaluating the model's performance included accuracy and false alarm rates. For the binary classification, the CNN-FL model achieved its highest accuracy rate at 99.20% and its lowest false alarm rate at 1.42%. For the multi-class classification, the highest accuracy rate achieved was 97.60%, and the lowest false alarm rate achieved was 0.55%. These results underscored the model's effectiveness at detecting and classifying cyber threats in IoHT devices. Furthermore, the performance of the CNN-FL model was compared to centralized deep learning models (CNN, DNN, and RNN), and the results showed that the federated learning approach held high performance while offering significant privacy advantages.

Table of Contents

Dedication ..... **iv**

Acknowledgements ..... **v**

Abstract of Praxis ..... **vi**

List of Figures ..... **xii**

List of Tables ..... **xiii**

List of Equations ..... **xiii**

List of Acronyms ..... **xvi**

Chapter 1—Introduction **1**

1.1 Background 1

1.2 Research Motivation 2

1.3 Problem Statement 2

1.4 Thesis Statement 3

1.5 Research Objectives 4

1.6 Research Questions and Hypotheses 4

1.6.1 Research Questions 5

1.6.2 Research Hypothesis 5

1.7 Scope of Research 5

1.8 Research Limitations 6

1.9 Organization of Praxis 7

Chapter 2—Literature Review **9**

2.1 Introduction 9
2.2 Overview of Internet of Healthcare Things (IoHT) and Cybersecurity 9
2.2.1 Integration of IoT in Healthcare 10
2.2.2 Cyber Threats on the Internet of Healthcare Things (IoHT) Devices ... 10
2.2.3 Conventional Cybersecurity Solutions and Mitigation Strategies for ... 13
IoHT Devices and Their Limitations 13
2.3 Machine Learning-based Cyber Threat Detection for IoHT Devices 14
2.4 Deep Learning-based Cyber Threat Detection for IoHT Devices 17
2.5 Conventional Neural Networks and Federated Learning-based Models in
Cyber Threat Detection 20
2.5.1 Basics of CNN Architecture and Applications 20
2.5.2. CNN and Cybersecurity 21
2.5.3 Introduction to Federated Learning 23
2.5.4 Existing Federated Learning-based Cyber Threat Detection Solutions. 26
2.6 Gaps in the Existing Literature 29
2.7. Conclusion 32
Chapter 3—Methodology 33
3.1 Introduction 33
3.2 Dataset Description 34
3.3 Loading the Dataset 34
3.4 Exploratory Data Analysis 35
3.5 Data Preprocessing 36
3.5.1 Data Cleaning 36

3.5.2 Categorical Data Encoding 37
3.5.3 Data Standardization 37
3.5.4 Stratified K-Fold Cross-Validation and Data Splitting 38
3.5.5 Balancing the Dataset 39
3.6 Building Machine Learning Models 40
3.6.1 CNN-Federated Learning Approach 40
3.6.2 Centralized Deep Learning Models 45
3.7 Model Evaluation 47
Chapter 4—Results 49
4.1 Introduction 49
4.2 Description of the ECU-IoHT Dataset 49
4.3 Exploratory Data Analysis 51
4.4 Federated Learning Aggregation Method Selection 59
4.5 Model Evaluations 60
4.5.1 CNN-FL for the Binary Classification Approach 60
4.5.2. CNN-FL for the Multi-Class Classification Approach 61
4.5.3 Centralized Deep-Learning (DL) Models 62
4.6 Model Comparison and Analysis 76
4.7 Implications for Healthcare IoT Security 77
Chapter 5—Discussion and Conclusions 79
5.1 Discussion 79
5.1.1 RQ1 and H1: Discussion 79
5.1.2 RQ2 and H2: Discussion 80

Evaluation Metrics 81

5.1.3 RQ3 and H3: Discussion 82

5.2 Conclusion 83

5.3 Contributions to Body of Knowledge 84

5.4 Recommendations for Future Research 85

References 87

List of Figures

Figure 2-1: Basic CNN Architecture (Montero et al., 2023) 21

Figure 2-2: Federated Learning and its Training Process (Rahman et al., 2023) 24

Figure 4-1: Distribution of the Target Feature "Type" 50

Figure 4-2: Distribution of Individual Features of the Dataset 55

Figure 4-3: Boxplot of Individual Features of the Dataset 56

Figure 4-4: Correlation Heatmap of the ECU-IoHT Dataset Features 57

Figure 4-5: Scatter Plots of the ECU-IoHT Dataset Features 59

Figure 4-6: CNN for Binary Classification Confusion Matrix 64

Figure 4-7: RNN for Binary Classification Confusion Matrix 66

Figure 4-8: DNN for Binary Classification Confusion Matrix 68

Figure 4-9: CNN Multi-Class Classification Confusion Matrix 71

Figure 4-10: RNN Multi-Class Classification Confusion Matrix 74

Figure 4-11: DNN Multi-class Classification Confusion Matrix 76

List of Tables

Table 4-1: Count of "Type of Attack" 50

Table 4-2: Summary Statistics for ECU-IoHT Dataset Feature 52

Table 4-3: Dataset Features and Types 53

Table 4-4: Count of NA Values in the Dataset 54

Table 4-5: Performance Results for FL Aggregation Methods 60

Table 4-6: CNN-FL Binary Classification Results Summary for 15, 10, and 5 clients ... 61

Table 4-7: CNN-FL Multi-Class Classification Results Summary for 15, 10, and 5 Clients 62

Table 4-8: CNN Binary Classification Results Summary 63

Table 4-9: Training Details for CNN Binary Classification 63

Table 4-10: RNN Binary Classification Summary 65

Table 4-11: Training Details for RNN for Binary Classification 65

Table 4-12: DNN Binary Classification Result Summary 67

Table 4-13: Timing Details for DNN Binary Classification 67

Table 4-14: CNN Multi-Class Classification Result Summary 70

Table 4-15: Timing Details for CNN Multi-Class Classification 70

Table 4-16: RNN Multi-Class Classification Result Summary 73

Table 4-17: Timing Details for RNN Multi-Class Classification Result 73

Table 4-18: DNN Multi-class Classification Result Summary 75

Table 4-19: Timing Details for DNN Multi-class Classification 76

Table 5-1: CNN-FL Binary and Multi-Class Classification Result Summary for 15, 10, and 5 Clients 81

List of Equations

Equation 3-1: Accuracy 48

Equation 3-2: Precision 48

Equation 3-3: Recall 48

Equation 3-4: F1-Score 48

Equation 3-5: False Alarm Rate 48

List of Acronyms

ANN	Artificial Neural Network
ARP	Address Resolution Protocol
CNN	Convolutional Neural Network
CNN-FL	Convolutional Neural Network-Federated Learning
DL	Deep Learning
DoS	Denial of Service
DNN	Deep Neural Network
DNS	Domain Name Service
DT	Decision Tree
EHR	Electronic Health Records
FAR	False Acceptance Rate
FedAvg	Federated Average
FedSGD	Federated Stochastic Gradient
FedProx	Federated Proximal
FL	Federated Learning
GDPR	General Data Program Regulation
HIPAA	Health Insurance Portability and Accountability Act
IoT	Internet of Things
IoHT	Internet of Healthcare Things
IoMT	Internet of Medical Things
IDS	Intrusion Detection System

LSTM	Long Short-Term Memory
MFA	Multi-factor Authentication
ML	Machine Learning
MSSQL	Microsoft Structured Query Language
NB	Naïve Bayes
NIID	Non-independent identically distributed
ReLu	Rectified Linear Unit
RNN	Recurrent Neural Network
RQ	Research Question
SDN	Software Defined Network
SMOTE	Synthetic Minority Over-sampling Technique
SVM	Support Vector Machine

Chapter 1—Introduction

1.1 Background

The "healthcare industry has undergone a technological transformation with the integration of Internet of Things (IoT) devices" (Alalhareth & Hong, 2024) for providing healthcare services, which has led rise to the Internet of Healthcare Things (IoHT). This shift holds a great opportunity to fundamentally revolutionize patient care and data management in healthcare settings (Poenicke et al., 2019). These devices composing the IoHT comprise various devices and sensors that collect and transmit valuable and sensitive healthcare data (Ahmad & Siddiqui, 2022). These IoHT devices have the potential to improve and optimize healthcare operations and decrease expenses (Perera et al., 2013). However, the proliferation of IoHT devices in the healthcare environment has created many challenges in cybersecurity for the healthcare industry.

The healthcare industry holds a large amount of patient data, making it a lucrative target for criminals seeking profit through cyber means. Malicious actors increasingly target healthcare organizations with various cyber threats, including ransomware attacks, "data breaches, and denial-of-service (DoS) attacks" (Kaur et al., 2024). In the case of IoHT, the consequences of cybersecurity breaches can be catastrophic, as they may impact patient safety, compromise the confidentiality of medical records, and disrupt critical healthcare services (Kruse et al., 2017). In 2021, the Diego Center for Healthcare Security in the USA succumbed to ransomware attacks causing the most severe disruption the center had ever seen (Ferrag et al., 2021). For nearly a week, the healthcare facility's operation was halted as the enterprise struggled to identify the malware.

1.2 Research Motivation

The strong commitment to finding solutions for the security and privacy issues in IoHT devices motivates this praxis. Due to the continued reliance of healthcare systems on IoT devices for timely and efficient treatment, there is an absolute need to safeguard patient records and medical systems. The increase in frequency and complexity of cyberattacks on healthcare organizations demonstrates the urgency of a complex machine-learning model capable of detecting and classifying cyber-attacks to save patient data privacy.

Conventional methods of cyber threat detection, such as signature-based techniques and anomaly detection, often lag behind sophisticated and ever-evolving threats. The utilization of federated learning methods in the cyber security of the healthcare IoT ecosystem can be tremendously beneficial. “Federated learning is a privacy-preserving machine learning technique wherein multiple decentralized devices jointly train a global machine learning model while keeping their local data” (Babbar, et al., 2023). Healthcare IoT deals with private and secure data; hence, federated learning is appropriate in such domains. Through federated learning, a model can be trained without centralizing the private data. Due to this advantage, it avoids the risk of exposing sensitive patient data, potentially reducing serious healthcare data breaches and staying compliant with healthcare data regulations.

1.3 Problem Statement

The increasing adoption of IoT devices and their inherent vulnerabilities have made them attractive targets for cybercriminals (Sue, 2023), resulting in an average cost of nearly 11 million dollars per breach in the healthcare industry (Adams, 2023).

Rapid deployment of Internet of Things (IoT) devices in healthcare has rendered the sector highly susceptible to cyberattacks. IoHT devices are repositories of extensive patient information, resulting in healthcare institutions becoming a constant target for cyber threats, such as ransomware attacks. From a public health point of view, cyber-attacks on IoHT devices can have serious implications, including harm to patients, breaches of medical privacy, and compromises to continuously deliver necessary healthcare services.

1.4 Thesis Statement

A Convolutional Neural Network (CNN)-federated learning-based intrusion detection system will detect and classify cyber threats in Healthcare Internet of Things devices while preserving privacy of patients' sensitive data.

The growing prevalence of "IoT applications in healthcare" has led to an improvement in patient care (Saleh et al., 2024). However, it has also intensified concerns regarding the privacy and security of sensitive health data. This praxis aims to solve this vital problem by proposing a novel CNN-Federated Learning-based Intrusion Detection System (IDS) for IoHT devices.

The primary goal of the suggested model is to identify and categorize cyber threats in IoHT domains through the power of CNN, discerning deep patterns in data (Balasubramaniam et al., 2023), and using FL techniques for decentralized model training. By combining the use of CNN with FL, the preservation of the privacy of patient data will be ensured. The model can be trained by bringing together the multiple distributed datasets without exposing the individual health records of a patient.

1.5 Research Objectives

This research aims to enhance the security and privacy of healthcare services provided by IoHT devices by architecting a hybrid deep learning (DL) model using federated learning techniques. Federated learning, a decentralized machine learning approach, offers promising prospects in addressing healthcare IoT's unique security and privacy challenges (Odeyemi et al., 2024, p. 2024). This research aims to:

- Develop a hybrid CNN-federated learning model to enhance the identification and categorization of cyber threats in IoHT devices.
- Evaluate the performance of the hybrid CNN-Federated learning model using an IoHT dataset.
- Evaluate the proposed hybrid model's ability to identify and categorize intrusions for different attacks using the following metrics: accuracy, precision, recall, F1-score, and false alarm rate (FAR). These metrics are used to compare the hybrid model with the existing DL models such as CNN, Recurrent Neural Network (RNN), and Deep Neural Network (DNN) intrusion detection systems.

1.6 Research Questions and Hypotheses

The research questions and hypotheses of this research are to determine whether a CNN-federated DL-based model can be built to detect and classify cyber threats in IoHT devices while maintaining patients' privacy. In addition, the questions and hypotheses will examine which federated learning (FL) aggregation methods will yield better performance results.

In order to design a model, the following research questions and hypotheses will serve as a guide for this research.

1.6.1 Research Questions

This praxis will address the following key research questions (RQ):

RQ1: Which federated learning aggregation method, out of Weighted Federated Average (Weight FedAvg), FedSGD, and FedProx, will achieve the highest accuracy in detecting and classifying cyber threats while preserving data privacy in IoHT devices?

RQ2: Can a hybrid CNN-federated learning-based model be built to detect and classify cyber threats while preserving patients' privacy in IoHT devices?

RQ3: Will the proposed model perform better in accuracy, precision, recall, and F1 score than other deep learning-based algorithms, such as CNN, RNN, and DNN, to detect and classify cyber threats while preserving privacy in IoHT devices?

1.6.2 Research Hypothesis

H1: The Weight FedAvg will achieve a higher accuracy than the FedSGD and FedProx in detecting and classifying cyber threats while preserving data privacy in IoHT devices.

H2: A hybrid CNN-federated learning-based model can be built to detect and classify cyber threats while preserving patients' privacy in IoHT devices.

H3: CNN-Federated learning will perform at a higher accuracy, precision, recall, F1 score, and lower false acceptance rate (FAR) than the other deep learning-based algorithms (CNN, RNN, DNN) to detect and classify cyber threats while preserving privacy in IoHT devices.

1.7 Scope of Research

The scope of this praxis covers cyber-attack detection and classification within the dynamic landscape of IoHT devices. At the core of it, this praxis is built around a dataset known for its richness and relevance in harvesting the multifaceted nature of

cyber threats in IoHT devices – the ECU-IoHT dataset. This dataset represents a wealth of diverse data sources, ranging from network traffic patterns to device communications, vital for unraveling the complexities inherent in safeguarding IoHT ecosystems from malicious activities.

Additionally, a pivotal aspect of this praxis involves subjecting the proposed model to rigorous performance evaluations conducted on a meticulously constructed subset of the ECU-IoHT dataset. The overarching objectives of the model are twofold: to achieve a higher detection accuracy, thereby bolstering the IoHT infrastructure's resilience against cyber intrusions, and to minimize false alarms, thereby averting unnecessary disruptions to critical healthcare operations).

Moreover, the model is engineered to be adaptable and able to accommodate both binary and multi-class classification of cyber threats, enhancing its versatility and utility across various IoHT contexts. Through this multifaceted approach, this praxis strives to provide valuable insights and solutions to fortify the cybersecurity posture of IoHT ecosystems, ultimately fostering safer and more resilient healthcare delivery systems.

1.8 Research Limitations

The goal of this praxis is to create an efficient and accurate system to detect and classify cyber-attacks in IoHT devices, particularly with a pre-dominant concentration on protecting sensitive patient information with privacy and integrity of sensitive patient information. While preventive measures are very important parts of cyber security frameworks, they are out of the scope of this research. Instead, the evaluation within this praxis concentrates on the performance of the proposed model by utilizing the ECU-IoHT dataset, which represents sample scenarios in IoHT.

Recognizing that the model's results developed in this praxis may have considerable significance in the field, it is crucial to acknowledge that IoHT environments have such a wide diversity of problems that the generalization of the results to all IoHT environments may be limited by the specific nature of the dataset and experimental conditions. This is to highlight the need for continued and contextualized research to address the diverse array of challenges present in IoHT environments.

Additionally, this praxis recognizes the broader legal and ethical considerations about data privacy and compliance within IoHT ecosystems. Although these concerns are paramount in shaping the landscape of cybersecurity in healthcare, they fall beyond the immediate scope of this study, signaling opportunities for future research across interdisciplinary domains.

1.9 Organization of Praxis

The praxis is comprised of five main chapters. These are:

Chapter 1 provides the background and research motivation behind this praxis, followed by the problem and thesis statements, the research motivation, objectives, research questions, hypotheses, scope, and limitations.

Chapter 2 provides a comprehensive literature review, offering insights into IoT in healthcare, security and privacy challenges, Federated Learning, and related work. This chapter also highlights the gaps in the literature and the need for the solution proposed in the praxis.

Chapter 3 explains the research methodology used during this research such as, the exploratory data analysis, data preprocessing, model development, and evaluation.

Chapter 4 displays the results of the proposed model. In this praxis, the results will focus on whether a hybrid CNN-Federated Learning model can detect and classify cyberattacks IoHT devices while maintaining the privacy of patient data. This chapter will also examine the performance of the proposed solution with the different DL models.

The final chapter, Chapter 5, discusses the results, challenges, limitations, and direction for future work.

Chapter 2—Literature Review

2.1 Introduction

This chapter reviews existing literature related to cyber threat detection on the Internet of Healthcare Things (IoHT), deep learning models, and federated learning models. Its structured into six primary sections. Section 2.2 provides a general description of IoHT and cybersecurity, including how IoT is being integrated with healthcare, the cyber threats in IoHT devices and the conventional methods to combat them. Section 2.3 delves into the cyber threat detection in IoHT devices that is based on machine learning, while Section 2.4 looks at the cyber threat detection in IoHT devices that is based on deep learning. Section 2.5 of this document is dedicated to introducing federated learning, its advantages and challenges, and its application in healthcare. Federated learning-based cyber threat detection in IoT devices is reviewed in this section, as well. In summary, the chapter concludes with literature review, summarizing the research gaps in Section 2.6 and laying the groundwork for this dissertation in Section 2.7.

2.2 Overview of Internet of Healthcare Things (IoHT) and Cybersecurity

The introduction of IoHT devices in healthcare settings has significantly revolutionized and modernized patient care and monitoring while raising major cybersecurity challenges regarding the protection of sensitive data and integrity of the entire healthcare system. This section provides a comprehensive overview of IoHT technologies, their applications in healthcare settings, and the urgent solutions for better cybersecurity.

2.2.1 Integration of IoT in Healthcare

In recent years, hospital systems have integrated IoT devices into their online healthcare applications and services to facilitate the seamless exchange of patient-specific health information and records, whether the patient is at home or receiving care in a hospital setting (Abouzakhar et al., 2017). Consequently, this technological transformation has given rise to the IoHT, a subdomain of IoT designed explicitly for healthcare applications. IoHT comprises many "devices, such as wearable fitness trackers, medical sensors, smart medical devices, and electronic health records (EHR) systems, which collect and send essential healthcare information about a patient" (Dang et al., 2019).

Although IoHT holds the potential to reshape healthcare, it also poses unpresented cybersecurity challenges. IoHT devices are often connected and networked, making them vulnerable to various cyber threats.

The healthcare sector is an enticing target for malicious actors due to its wealth "of sensitive patient data, including medical records, personal information, and financial data" (Sittig & Singh, 2016). The ramifications of a cyber breach in a healthcare context can be very devastating, affecting patient safety, data privacy, and the integrity of healthcare services (Kruse et al., 2017).

2.2.2 Cyber Threats on the Internet of Healthcare Things (IoHT) Devices

Healthcare organizations are continually grappling with the challenge of addressing advanced and complex cyber threats. The healthcare sector is particularly critical, necessitating specialized approaches to prevent, identify, and evaluate attacks (Goud, 2019). Djenna et al. (2021) reported that "according to Vectra Networks' quarterly

post-intrusion analysis report for the first quarter of 2017, healthcare was the most frequently targeted sector for cyber-attacks". For example, 86% of the attacks have been found in "the implementation of IoT" (Elgayar et al., 2023). The effects of a cyber-attack on an IoT-enabled healthcare system could be serious and widespread, leading to "financial loss, operational disruption, equipment failure, and most critically, the loss of patients' lives" (Djenna et al., 2021). Considering these risks, it is worth exploring some of these cyber-attacks to identify their inherent vulnerabilities, as well as associated risks within IoT-based healthcare.

Denial of Service (DoS) attacks represent one of the most prevalent threats facing IoHT devices, posing significant challenges to the reliability and functionality of these critical systems. In a DoS attack, malicious actors inundate targeted IoT devices with excessive requests, overwhelming their processing capabilities and exhausting available resources. This barrage of requests impedes the device's ability to respond to legitimate user requests, rendering it unresponsive or severely degraded performance (Lyell et al., 2021).

The disruptive impact of DoS attacks on IoHT devices is particularly concerning due to the critical nature of the services they support. Medical devices and systems rely on seamless communication and real-time data exchange to deliver vital healthcare services, such as patient monitoring, diagnostics, and treatment delivery. However, the lack of synchronization in communications exacerbated by DoS attacks can lead to disruptions in these essential services, and negatively impact the quality and care.

Another type of attack that IoHT devices are subject to is the replay attack. "A replay attack is a security breach in which unauthorized data is stored" and then

transmitted to the receiver to trap them in unauthorized actions such as false authentication or verification or duplicate transactions (Chakraborty, et al., 2022). The attacker aims to gain the receiver's trust and often uses a message commonly used in the access process (Behrooz & Marsh, 2016). Relying solely on basic authentication methods, such as login activity without session key generation, is insufficient to ensure security. A replay attack can be prevented by limiting unauthorized access to the system (Butt et al., 2019).

Implementing robust access control mechanisms is essential for thwarting unauthorized access to sensitive systems or data. This entails deploying authentication measures like passwords, biometrics, or “multi-factor authentication (MFA) to restrict the system’s access solely to authorized users” (Yaacoub et al., 2022). Additionally, encrypting transmitted data is a layer of protection against replay attacks; even if intercepted, encrypted data remains indecipherable and tamper-proof without the requisite decryption key.

The subsequent threat to IoHT devices explored in this section pertains to ransomware attacks, a distinctive form of malware notorious for impeding hospital organizations' access to vital system components, posing significant concerns regarding hospital data security. Ransomware encrypts data, effectively barring healthcare personnel from accessing crucial health information and databases, potentially disrupting critical healthcare operations (Thamer & Alubady, 2021). In the event that an organization within the hospital sector is incapable of accessing its own health information system, it could lead to delays or hinder the provision of care.

2.2.3 Conventional Cybersecurity Solutions and Mitigation Strategies for IoHT Devices and Their Limitations

Data security represents one of the core mandates for healthcare institutions to safeguard patient data by securing IoT devices. These protective measures give hospitals more significant milestones in protecting the institution's reputation. This section explores numerous solutions that have been developed over the years to tackle the security concerns posed by IoHT devices, thereby reducing the likelihood of cyberattacks (Al-Haija et al., 2021).

One solution recommended as best practice is to implement distributed systems. Most denial-of-service attacks occur due to the central server's lack of appropriate synchronizations. Therefore, implementing a distributed system allows overwhelming request workloads to be distributed to different servers (Hagras et al., 2023). This method has been the most efficient mitigation approach for a long time, ensuring that the network devices efficiently help implement the security of the network systems.

Another mitigation approach is to develop comprehensive user guidelines to heighten security awareness. It is crucial to provide clear and concise instructions on protecting IoT devices. This includes educating users on the potential threats that can affect their devices and how to prevent them. Additionally, organizations can develop robust training programs to enhance and cultivate security awareness among employees, which will essentially include how to create strong passwords, change the passwords regularly, and training on how to identify spam e-mails, as well as third-party apps that might compromise IoT security. By adhering to these tenets and following best practices, users reduce the danger of IoHT attacks and data breaches (Tawalbeh et al., 2020).

Another security practice often used is the implementation of roles and privileges. This approach requires that different users have well-spelled-out roles in the system, which can reduce the number of trusted insiders. In any organization, the responsibility of protecting organizational data largely relies on trusted insiders (Hu et al., 2021).

Conventional cybersecurity approaches face numerous challenges in dealing with cyber breaches in IoHT devices. The intricate and diverse nature of IoT ecosystems in healthcare settings presents a significant barrier, making it difficult to thoroughly monitor and safeguard every device. Furthermore, numerous IoHT devices exhibit inherent vulnerabilities due to inadequate built-in security mechanisms, leaving them susceptible to exploitation by malicious actors (Bera et al., 2017). Additionally, the speed of digital innovation at times outpaces the responsiveness of traditional security measures, leaving healthcare systems vulnerable to emerging threats (Bera et al., 2017). These limitations highlight the urgent need for innovative cybersecurity strategies targeted specifically to IoHTs.

2.3 Machine Learning-based Cyber Threat Detection for IoHT Devices

Traditional and common security approaches are less effective in the IoT environment due to the specific characteristics of these "devices, such as their scalability, processing power, memory, and power resource restrictions" (Hussain et al., 2021). To overcome this issue, machine learning-based IDS are developed. In this section, machine learning-based cyber threat detection techniques developed for IoHT devices against cyber-attacks are studied.

Binbusayyis et al. (2022) conducted a research project that focused on using different machine learning techniques like NB, KNN, DT, ANN, and SVM to detect and

prevent intrusion on the Internet of Medical Things (IoMT) network. In the study, the 2018 Bot-IoT dataset was used to explore the different machine-learning approaches to "comprehend the best practice when it comes to finding the intrusion of the networks in IoMT" (Binbusayyis et al., 2022). Their research aimed to determine the most suitable machine learning model capable of enhancing the security of the IoMT networks, ensuring the privacy and integrity of medical records in IoT networks.

Results showed that DT demonstrated the most effective detection capabilities across all three evaluation measures. It achieved 100% accuracy (ACC), 100% detection rate (DR), and 12.00% false alarm rate (FAR), which is the ratio of misclassified normal instances on the imbalanced Bot-IoT datasets. It also achieved 100 % ACC, 100% DR, and 0.00% FAR on the balanced Bot-IoT datasets (Binbusayyis et al., 2022).

Thamilarasu et al. (2020) as cited in Akshay Kumaar et al. (2022), designed an intrusion detection system for securing the network of connected medical devices on the IoMT. The models they used for their intrusion detection were based on machine learning algorithms to detect network-level intrusions and anomalies in sensor data, including SVM, DT, NB, KNN, and RF (Thamilarasu et al., 2020). The authors simulated a hospital network topology and performed experiments on subsets of the IoMT to validate the system's accuracy of 99.80% and 97.93% for "network and device intrusion detection" (Thamilarasu et al., 2020). They stressed the importance of addressing security concerns in the IoMT and proposed using mobile agents for intrusion detection (Thamilarasu et al., 2020).

Basharat et al. (2022) conducted an in-depth analysis of various ML methods for intrusion detection in IoHT devices. The goal of this paper was to measure the

effectiveness of various machine learning techniques such as SVM, Random Forest (RF), Bagging, and AdaBoost in safeguarding IoHT devices against security breaches. By examining these techniques, the study sought valuable insights into which approaches are best suited for enhancing the security of smart healthcare systems, protecting sensitive patient data, and maintaining the reliability of healthcare services (Basharat et al., 2022). The study was evaluated using the UNSW-NB15 network intrusion benchmark dataset, demonstrating its ability "to detect network intrusion with the highest accuracy" rate of 95.32% using the AdaBoost classifier (Basharat et al., 2022).

Tauqeer et al. (2022) investigated "machine-learning techniques for detecting cyber-attacks" on the IoMT. The authors evaluated three "machine learning algorithms—RF, Gradient Boosting, and SVM"— to detect cyberattacks. These models have shown particular efficacy in detecting cyberattacks and have thus been evaluated on the WUSTL EHMS 2020 dataset, which contains a variety of attack types, including main in-the-middle, data injection, and spoofing attacks (Tauqeer et al., 2022). According to the evaluation of the presented machine-learning models, Random Forest yielded an accuracy rate of 96.92%, the Gradient Boosting model resulted in an accuracy rate of 96.53%, while an accuracy rate of 95.85% was achieved by SVM (Tauqeer et al., 2022).

Lee et al. (2021) proposed a novel M-IDM approach for identifying security breaches in healthcare Internet of Things (IoT) networks. M-IDM employed multi-classification techniques to analyze network traffic, allowing it to distinguish various intrusions and protect the "confidentiality and reliability of sensitive patient data in the" healthcare IoT ecosystem (Lee et al., 2021). The authors demonstrated that their proposed

model achieved a high accuracy rate, ranging from 94.49% to 98.82% in all classes (Lee et al., 2021).

As discussed in this section, many studies were presented to demonstrate that ML techniques can be used to build intrusion detection systems to detect and prevent cybersecurity breaches in the healthcare environment. While the different machine learning-based cyber threat detection techniques have shown a high accuracy rate, they have not addressed patient data privacy, which is a major concern in the healthcare sector. This is due to its potential to compromise patient confidentiality, violate regulatory compliance, erode trust and patient confidence, and raise ethical dilemmas (Okey et al., 2022).

2.4 Deep Learning-based Cyber Threat Detection for IoHT Devices

Deep learning-based cyber threat detection systems have been developed to address the concerns and limitations of machine learning techniques for cyber threat detection. This section will explore deep learning-based cyber threat detection for IoHT devices.

Akshay Kumaar et al. (2022) proposed a new hybrid framework called "ImmuneNet" specifically intended for intrusion detection in healthcare systems. The framework leveraged deep learning methods to increase accuracy and capability, combining multiple feature engineering techniques, oversampling approaches, and hyperparameter optimization methods. The proposed framework is compared with various machine learning algorithms using cyber-attack data from the "Canadian Institute for Cybersecurity's Intrusion Detection System 2017, 2018, and Bell DNS 2021 datasets" (Akshay Kumaar et al., 2022). The average results obtained in the CIC Bell DNS 2021

dataset are 99.19% for accuracy, 99.22% for precision, 99.19% for recall, and 99.21% for AUC-Roc in the proposed framework (Akshay Kumaar et al., 2022).

Kim et al. (2016) developed an intrusion detection system (IDS) model using a deep learning approach by adopting a Long Short-Term Memory (LSTM) architecture into a Recurrent Neural Network (RNN)" to classify the patterns of an attack. The model was "trained using the KDD Cup 1999 dataset. The results revealed that it achieved an average detection rate (DR) of 98.87% among the total attack instances, whereas the average FAR was 10.03% (Kim et al., 2016).

Vijayakumar et al. (2023) developed a "cyber-attack detection system based on deep neural networks utilizing the latest ECU-IoHT". The proposed system aimed to identify "cyber-attacks on the Internet of Health Things environment" and achieved performance accuracy, with an average of 99.85% (Vijayakumar et al., 2023). Additionally, "the system has a false positive rate of 1.00% and an average area under the receiver operator characteristic curve of 99.00%" (Vijayakumar et al., 2023).

In their study, Saheed and Arowolo (2021) devised an effective system to detect cyber-attacks within the Internet of Medical Things (IoMT) by using Deep Recurrent Neural Network (DRNN) and machine learning techniques, including random forest (RF), decision tree (DT), KNN, and ridge classifiers. The NSL-KDD dataset was utilized to conduct the experimental work. The DRNN model produced a higher accuracy rate of 99.76% (Saheed & Arowolo, 2021).

In their paper, Judith et al. (2023) proposed a way to spot malicious software on the IoMT communication system using immediately collected data from the WUSTL-EHMS dataset. The authors employed PCA to reduce the feature number and constructed

a Multi-layer Perceptron for categorizing unexpected cyber-attacks (Judith et al., 2023). The evaluation of the proposed model indicated that the MLP achieved a better performance than other classifiers tested, obtaining an accuracy rate of 96.39% and briefly reducing the time complexity (Judith et al., 2023).

An effective and accurate intrusion detection system for the Internet of Medical Things (IoMT) was implemented by Chaganti et al. (2022) by proposing a particle swarm optimization deep neural network (PSO-DNN). To verify the performance of the proposed solution, the WUSTL EHMS 2020 Dataset for IoMT cybersecurity research has been employed (Chaganti et al., 2022). Their results revealed that the accuracy rate in detecting network intrusions is 96.00%, which is slightly more than other machine learning solutions (KNN, DT). To identify the best model for network intrusion detection in IoMT, the authors compared various machine learning (ML) and deep learning (DL) techniques. According to their findings, the accuracy rate of the ML techniques (LR, KNN, DT, AdaBoost, RF, DT) is between 91.60% and 95.30%, while the accuracy of the DL techniques (DNN, CNN, LSTM) is between 95.20% and 95.70% (Chaganti et al., 2022).

A new approach to anomaly detection based on deep neural network (DNN) for IoT network architectures was proposed by Ahmad et al. (2021), aimed at detecting complex patterns within IoT network flows and distinguishing normal network flows from anomalies. The proposed model was tested on the IoT-Botnet 2020 dataset and achieved a detection accuracy of 99.01% and a false alarm rate of 3.90% (Ahmad et al., 2021). In future research, the authors proposed adapting their multiclass classification scenarios to specifically categorize the flagged anomaly.

2.5 Conventional Neural Networks and Federated Learning-based Models in Cyber Threat Detection

This praxis aims to build a model that combines Convolutional Neural Networks (CNNs) with federated learning (FL) methods. This innovative approach combines CNNs' exceptional feature extraction and pattern recognition capabilities with the privacy-preserving features of FL.

2.5.1 Basics of CNN Architecture and Applications

Convolutional Neural Networks CNNs have become an essential part of modern deep learning, particularly in the area of computer vision, because of their substantial achievements on various image analysis benchmarks, and include convolutional layers, pooling layers, and fully connected layers (Maurício et al., 2023). As the principal building blocks in CNNs, convolutional layers extract the complex localized spatial hierarchies by evaluating the summation of the input data across the receptive fields and applying a nonlinear operation to obtain the output feature maps (Krizhevsky et al., 2017).

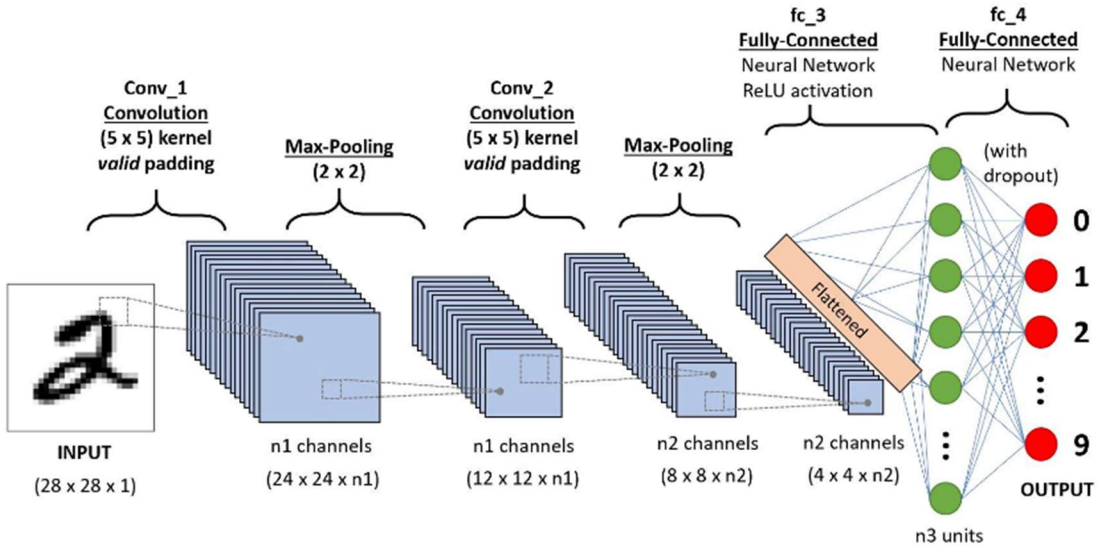

Figure 2-1: Basic CNN Architecture (Montero et al., 2023)

CNN has been used to identify objects in real-time videos through image analysis and feature extractions (Sharma et al., 2018). In CNNs, the most significant features are weight sharing and hierarchical connections with automatic self-training. Semi-connected and fully connected layers within CNNs fulfill distinct roles, creating a conducive environment for the feed-forward training process and the backward propagation of errors.

2.5.2. CNN and Cybersecurity

There are different approaches in which CNNs can be used to improve security. CNNs were initially created for image recognition tasks, but because of their propensity to efficiently learn hierarchical representations, they have also been applied in cybersecurity (Le et al., 2024). In the realm of cybersecurity, CNNs offer promising avenues for detecting and mitigating various types of threats, including malware detection, intrusion detection, and vulnerability assessment. The following are some of the methods in which CNN can be used to strengthen cybersecurity.

CNN has been used to detect information that has been embedded in images. This becomes a very suitable mechanism for eliminating possible attacks by malware as all the suspicious images can be identified and covert any malicious activities that might be in transit (Dixit & Silakari, 2021).

Additionally, CNN has been used to identify malware in IoT networks. Communication, especially through Android devices, is easily susceptible to malware attacks (Nedeljkovic & Jakovljevic, 2022). Moreover, CNN can be effectively used to address the challenges of possible attacks by predicting the probable cause of attacks (Al-Turaiki & Altwaijry, 2021)

Furthermore, CNNs have shown great promise in intrusion detection systems (IDS) due to their ability to automate feature extraction from network traffic data to detect anomalies. The research done by Kim et al. (2020) and Radford et al. (2015) illustrated that a CNN-based IDS has the capability to identify anomalous actions that could potentially lead to security attacks. Through real-time analysis of network traffic patterns, CNN-based IDS could be used as a warning system that prompts a preventive response or mitigation action before it is too late.

Moreover, CNNs have been utilized for finding and prioritizing potential security vulnerabilities in software systems. By analyzing code snippets or system configurations, CNNs can learn patterns indicative of vulnerabilities, thereby assisting security professionals in conducting comprehensive security audits and risk assessments (Qiang, 2022).

2.5.3 Introduction to Federated Learning

"Federated learning (FL) is designed to protect data privacy" (Wu et al., 2021) and is widely recognized as one of the most efficient ways of detecting attacks in IoHT traffic. FL also "ensures that the privacy and security of sensitive information are significantly enhanced by training models locally without transmitting private data to a central server" (Rahman et al., 2023), as captured in Figure 2-2. By keeping the training data on the local server, the chances of an attack are reduced, and if an attack happens, the damage that can be done is reduced compared to the one in the centralized area (Ghimire & Rawat, 2022). Localizing the data and directly training the model in the devices or servers where data are stored further reduces the risk of exposing sensitive information to potential attackers.

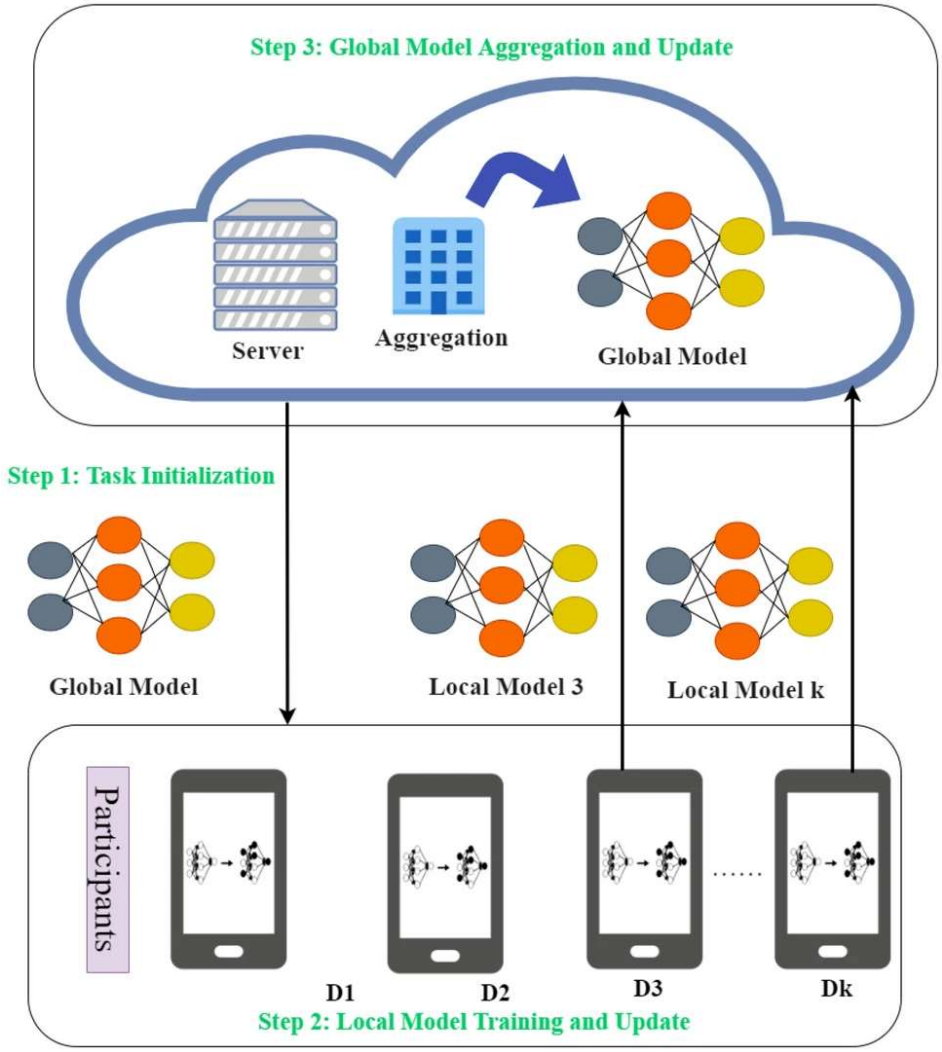

Figure 2-2: Federated Learning and its Training Process (Rahman et al., 2023)

Unlike conventional centralized machine learning approaches where data is "collected and processed at a single location, federated learning (FL)" (Ghadi et al., 2023) distributes the computational workload across multiple devices or servers, thereby decreasing the likelihood of successful cyber-attacks targeting a centralized data repository. This workload distribution ensures that even if a single device or server is compromised, the impact on overall system security is limited since the attackers would only gain access to a portion of the training data.

However, federated learning also presents some concerns. For example, automatic update information communicated to the central server could lead to security and privacy issues. If this data is not adequately secured during transmission, information distortion may occur and have negative consequences. The other issue is fault tolerance which is crucial to ensure efficient data communication in federated learning, particularly for IoT networks.

Despite these challenges and limitations, FL's emphasis on decentralized approach offers a notable advantage in safeguarding data privacy and confidentiality, which is very critical in medical environment where data confidentiality and patient privacy are paramount. By allowing machine learning models to be trained locally on individual devices and aggregating knowledge while keeping raw data decentralized, FL mitigates the risks associated with cyberattacks on IoHT networks.

Furthermore, FL allows for continuous learning and adaptation to diverse and evolving environments, a particularly valuable trait in the dynamic landscape of IoHT environments. Bonawitz et al. (2019) pointed out that FL's federated averaging algorithm facilitates model training across distributed devices, enhancing privacy without compromising performance. Although FL may present challenges such as communication overhead and potential model performance discrepancies across devices. These shortcomings can be addressed through optimization techniques and careful algorithm design. Despite these shortcomings, FL remains a promising solution for ensuring robust cybersecurity in healthcare IoT environments, striking a delicate balance between data privacy and model performance (Bonawitz et al., 2019).

2.5.4 Existing Federated Learning-based Cyber Threat Detection Solutions

Otoum et al. (2021) as cited in Si-Ahmed et al., (2024), conducted a study on building a federated transfer learning-oriented "intrusion detection system (IDS) for securing Internet of Medical Things (IoMT) networks and used a deep neural network (DNN) for collaborative training on the cloud and edge models". Evaluating with the CICIDS2017 dataset, the accuracy and detection rates as performance metrics were presented, and the experiment showed an accuracy rate of 95.14%, which suggested federal transfer learning model could outperform the conventional centralized learning base applications via the basic ML/DL algorithms in terms of scalability and incremental learning (Otoum et al., 2021).

Rashid et al. (2023) suggested that improving safety and privacy would involve an IoT IDS with federated machine learning. Their analysis focused on discovering undesirable intrusions and protecting IoT networks. Checking the present Edge-IIoT dataset, Rashid et al. (2023) displayed their trials with two typically used ML algorithms, CNN and RNN, using centralized and federated systems. According to the experiment, Rashid et al. (2023) stated that their planned federated learning technique hit an accuracy rate of 92.49% when contrasted to the 93.92% precision of the median-oriented ML models.

To enhance cybersecurity in IoT applications, Ferrag et al. (2021) conducted a thorough examination of federated deep learning approach through three different deep learning techniques: RNN, CNN, and DNN (Ferrag et al., 2021). The performance of these models was assessed using three datasets: the Bot-IoT, MQTTset, and TON_IoT datasets; and the results showed the highest accuracy rate of 96.76% for the RNN

classifier using the Bot-IoT dataset, 90.06% for the DNN classifier using the MQTTset dataset, and 99.98% for the RNN classifier using the TON_IoT dataset (Ferrag et al., 2021).

Furthermore, the federated learning model achieved the highest accuracy rate of 95.47% on the BoT-IoT dataset, 88.43% on the MQTTset dataset, and 98.86% on the TON-IoT dataset (Ferrag et al., 2021). The authors' research provided valuable insights into federated deep learning framework and their potential applications in the field of cyber security. Moreover, their reported results indicated that federated deep learning solutions exceeded the performance of standard/centralized ML methods by keeping the user's IoT data clear and improving the success of distinguishing the intrusion (Ferrag et al., 2021).

Duy et al. (2021) analyzed a federated learning (FL)-based invasion detection system for a software-defined network (SDN)-enabled industrial Internet of Things (IoT). The authors applied FL to their IDS model to preserve privacy during the models' training phase while maintaining the maximum intrusion detection efficiency, especially in industrial IoT using SDN. To evaluate the adequacy of their model, the authors used the CICDDoS2019 dataset, which comprises normal scenarios and DDoS attack scenarios that rely on real-world packet capture (PCAP) data flows (Duy et al., 2021). Results showed an accuracy rate of 98.20% in detecting synchronization (syn) attacks, 99.30% on Microsoft Structured Query Language (MSSQL), and 99.94% on NetBios attacks (Duy et al., 2021). Finally, the authors concluded that the application of federated learning can help to keep privacy with high accuracy of anomaly detection without impacting the confidentiality of sensitive network data.

Lee et al. (2023) proposed a CNN-federated learning-based intrusion detection model through which the full potential of federated learning is maximized. Their proposed model ensured data privacy while improving performance compared to existing algorithms. The authors evaluated their algorithm using the CICIDS 2017 dataset and a convolutional neural network-based intrusion detection model. Results showed an accuracy rate of 98.41% and an F1-Score of 96.10%, which outperformed the conventional algorithm regarding reduced training time and the number of weight transfers (Lee et al., 2023). While the proposed approach achieved a higher accuracy ratio, precision and recall scores were not computed. Furthermore, the CICIDS 2017 does not truly represent the IoHT characteristics and threats.

Making use of IoHT datasets is crucial for creating a machine-learning-based Intrusion Detection System (IDS) in the healthcare domain for various reasons. IoHT datasets have different particularities that differentiate them from datasets in other sectors and could influence the development and implementation of machine learning models in healthcare systems (Yuan et al., 2018). These datasets involve heterogeneous data sources, which include medical devices, Electronic Health Records (EHRs), wearable sensors, and patient monitoring systems. Therefore, using an IoHT dataset in this praxis would enable the identification of healthcare-specific threats such as medical device hijacking and the disclosure of private patient records.

In their work, Mosaiyebzadeh et al. (2023) were interested in training DNN-FL that would identify anomalies in IoHT traffic that could lead to security threats using performance metrics such as accuracy, precision, and recall. They validated their model performance using the wustl-ehms-2020 and ECU-IoHT datasets. Their model achieved a

91.40% accuracy in detecting attacks in the first dataset and 98.47% in the second (Mosaiyebzadeh et al., 2023). Finally, the authors suggested that future works should consider a hybrid Convolutional Neural Networks (CNN) – federated learning model "using larger datasets with different feature spaces" (Mosaiyebzadeh et al., 2023).

Federated learning represents a cutting-edge artificial intelligence (AI) technology that emphasizes the use of decentralized data learning and the extensive training of predictive models using sensitive private information of the user. The review of existing works showed that there is still work to be done on how federated learning could be used to build cyber threat detection solutions in IoHT devices.

2.6 Gaps in the Existing Literature

The literature review discusses a complete synthesis of the different solutions proposed for cyber-attack detection and classification in IoHT devices, according to the previous research. Although several significant contributions have been made in the field of cyber threat detection solutions based on ML/DL algorithms and techniques, several gaps still exist and need to be addressed in future research efforts.

The first research gap identified in this literature review is the limited use of the IoHT datasets in evaluating the performance of proposed solutions in the healthcare environment. IoHT datasets are comprehensive formats of the available healthcare resources (e.g., doctors, hospitals, rehabilitation centers, medical devices, sensors, and patients), which enable fast and efficient data exchange between them over the internet. This data may contain physiological measurements, patient health records, activity tracking data, etc. According to Sarker et al. (2023), the heterogeneity, high volume, and

dynamics of IoHT datasets appear to introduce security challenges beyond traditional security capabilities.

Additionally, these datasets are within the clinical context of patient care, dealing with interactions between medical devices, healthcare providers, and patients. They include various data sources like medical sensors, electronic health records (EHR), and diagnostic imaging systems, encapsulating the complexity of healthcare delivery. Thus, it is essential to use an IoHT-specific dataset since machine learning (ML)-based IDS are built to tailor the intricacy of healthcare IoT environments differently to detect a higher detection rate, influencing performance and adaptability requirements.

The review of literature further identified another gap, which is that there is a scarcity of machine learning-based intrusion detection solutions whose primary objective is to address privacy concerns in multi-class classification cyber threat detection models to identify various cyber-attacks in IoHT devices. Multi-class classification is an essential aspect of machine learning-based intrusion detection systems (IDS), which is fundamental to enhancing threat detection capabilities, improving incident response practices, and fortifying the cybersecurity posture of any organization.

As cyber threats come in various forms and levels of sophistication, multi-class classification allows IDSs to categorize attacks into distinct classes, providing a detailed and nuanced understanding of the threat landscape. This comprehensive approach also enables security analysts to make informed decisions regarding incident responses by allowing for prioritization based on the severity or type of attack. Furthermore, multi-class classification enables IDSs to learn from historical data and detect emerging attack

vectors, enhancing proactive detection capabilities, particularly for previously unseen or zero-day attacks (Sommer & Paxson, 2010).

Overall, multi-class classification provides a comprehensive view of the threat landscape, enhancing situational awareness for security operators and allowing for targeted security measures and resource allocation.

The third gap in this literature review is that a few of the existing solutions often suffer from high false alarm rates (FAR). Even though these FAR values are comparatively lower than the acceptable levels of false alarms for an IDS of less than 10.00% (Anuar et al., 2008), the opportunity still exists to reduce them even further.

A critical performance metric from the perspective of assessing the effectiveness of intrusion detection systems (IDS) based on machine learning is the false alarm rate, which indicates how well a system can distinguish benign activities from actual security threats. This was highlighted by Yadav and Sharma (2021), who noted that in the evaluation of an IDS, the false alarm rate is vital because too many false alarms can overwhelm the security personnel assessing the alerts, lead to alert fatigue, and ultimately result in real security breaches being overlooked.

Moreover, the high false alarm rate in machine learning-based IDSs for healthcare domains can have serious negative implications, including violations of confidentiality, degradation in the quality of patient care, erosion of trust, and wasted resources. To mitigate these drawbacks, it is crucial to implement reliable intrusion detection mechanisms that prioritize accuracy, reduce false alarms, and safeguard sensitive healthcare information effectively.

2.7. Conclusion

To address the literature review gaps discussed in section 2.6, this praxis aims to build a hybrid Convolutional Neural Network (CNN)-Federated Learning (FL) based model to improve the identification and categorization of cyber threats with data privacy protection in the IoHT devices. The proposed hybrid model benefits from the advantage of CNNs in recognizing patterns and extracting features, and it benefits from federated learning for maintaining the data privacy. This praxis also explores binary and multi-class classifications. Moreover, to evaluate the proposed model's performance, the praxis considers the FAR metric along with other evaluation metrics such as precision, recall, F1-score, and accuracy using the ECU-IoHT dataset which represents IoHT threats and characteristics.

Chapter 3—Methodology

3.1 Introduction

Given the increasing amount of private medical data transmitted over IT infrastructures, the healthcare sector and any company dealing with data from wearable devices has increasingly caught the eyes of malicious attackers. The challenges of protecting electronic healthcare data require building strong Intrusion Detection Systems (IDS) for Internet of Healthcare Things (IoHT) devices to secure the environment in which they operate. Understanding the unacceptability of directly collecting and processing this data for machine learning purposes, the idea of Federated Learning has gotten the attention of governmental bodies and healthcare organizations, where privacy preservation for users has become an issue.

Alternative to a centralized solution, federated learning is one of the privacy-preserved machine learning frameworks that analyze data without directly sharing it (Mosaiyebzadeh et al., 2023). In this praxis, a convolutional neural network in federated learning (CNN-FL) model is proposed to enhance the detection and classification of cyber threats in IoHT traffic. This model helps in addressing the security and privacy threats that are common concerns for healthcare organizations. The detection performance of the proposed CNN-FL is measured by different metrics like Accuracy and Precision, and the model has been validated by ECU-IoHT datasets.

This chapter is structured as follows: Section 3.2 describes the dataset used in this praxis. Section 3.3 depicts the process of loading to the analysis environment. Sections 3.4 and 3.5 discuss the exploratory data analysis and preprocessing processes. Section 3.6

describes the model development process, and section 3.7 describes the model performance metrics.

3.2 Dataset Description

The ECU-IoHT dataset, a unique and comprehensive resource, was developed by Ahmed et al. (2021). The dataset generation environment includes “Windows 10, Kali Linux, a mobile Wi-Fi hotspot, a wireless network adapter, and a Bluetooth adapter to establish connections to the Internet” (Algethami & Alshamrani, 2024). Additionally, a healthcare kit named MySignals is part of the environment, comprising various “components and multiple sensors designed to monitor and store patients' body biometric data, including temperature, blood pressure, and heart rate which then transmitted to the user's cloud” (Alghanmi, 2024). The dataset encompasses “seven features related to network data, such as source, destination, protocol, and the type of attacks. The ECU-IoHT dataset comprises 87,754 instances of normal activity and 23,453 attacks. The attacks include four different types: ARP spoofing, DoS attack, Nmap port scan, and Smurf attack” (Vijayakumar et al., 2023).

3.3 Loading the Dataset

The dataset used for this praxis, as discussed in Section 3.2, consists of deidentified patient records from a large healthcare system. It also has network data and cyber-attack types. The process of loading this dataset into our analysis environment on Google Colaboratory (Pro), which uses Python as a programming language, requires several meticulous steps. In the first step, the necessary libraries including their dependencies are imported: ‘pandas,’ ‘numpy,’ ‘sci-kit-learn,’ ‘matplotlib,’ and

'seaborn,' which are foundational for manipulating data, visualizing data, constructing machine learning models and neural networks.

Once the required libraries are installed, the dataset is loaded into the environment using the 'pandas. read_csv ()' data import function. By loading this dataset into our analysis environment, an initial investigation and analysis can reveal valuable insights into patient demographics, illness prevalence, and healthcare utilization patterns.

3.4 Exploratory Data Analysis

"Exploratory Data Analysis (EDA) is a set of methodologies used in a machine learning model to analyze, evaluate, and summarize the basic characteristics of a dataset" (Deming et al., 2018). The EDA steps aim to uncover anomalies or unusual patterns, as well as explore relationships among the features of the dataset. To achieve this goal, the EDA tasks performed in this praxis include verifying the number of counts and range of every feature in the ECU-IoHT dataset.

Furthermore, this praxis examines the distribution of each feature in the dataset by calculating fundamental statistical measurements such as the mean, the mode, the standard deviation, the minimum/maximum, and the percentiles. This praxis also checks for numerical features in the dataset, which can be very useful in building the machine learning model. Additionally, this praxis checks for missing values or outliers to be removed from the dataset because their presence could lead to an ineffective model's prediction and biases.

Moreover, this praxis performs a univariate analysis, which is one the common EDA techniques, to analyze the distribution of each individual feature by plotting the histograms and boxplots. This praxis also performs a bivariate analysis (two variables

analysis), which involves examining and analyzing the relationship between a pair of features. As a last step, this praxis builds the correlation heatmap, which explores the level of dependency between the different features in the dataset.

3.5 Data Preprocessing

"Preprocessing data is a crucial step in machine learning modeling, which helps avoid inconsistencies like errors or noise" (Obaid et al., 2019). In the process of creating an ML model, data cleaning, data transformation, and feature selection must be performed (Musleh et al., 2023).

3.5.1 Data Cleaning

"Data cleaning is an important step in preparing a dataset for analysis, including addressing missing values, outliers, and erroneous entries using imputation, outlier detection, and data validation" (Dasu & Johnson, 2003).

In most cases, missing values are the leading cause of poor-performing models. Filling those missing values with the imputation techniques is required.

Outliers can negatively affect the model obtained through machine learning and, accordingly, may yield awful predictions. Ensuring data consistency is of great importance since it will affect the model's training.

Some features will not affect the model's performance. For instance, the 'info' column, does not provide much valuable information about cyber threat detection. Therefore, it was dropped from the dataset using a drop function on the irrelevant features, which optimizes computational efficiency.

3.5.2 Categorical Data Encoding

Encoding categorical data is an important preprocessing step in machine learning as it facilitates the use of categorical variables as meaningful predictors in machine learning modeling. Most "machine learning algorithms can only operate on numerical data" (Wang, 2017). Therefore, they need to be transformed to numerical values before being used, which can be done through one-hot encoding (Cheng et al., 2017). Proper encoding categorical variables guarantees that the model can correctly interpret and utilize these features during training and prediction, leading to improved model performance across different tasks and datasets (Boriah et al., 2008).

During the preprocessing phase of the ECU-IoHT dataset, several transformations were applied to enhance its usability and facilitate subsequent analyses. For example, the "Time" column, which represents the timestamp of each record, was converted to DateTime format using the panda's library's "to_datetime" function, with the unit parameter set to seconds.

Furthermore, the analysis of the preprocessed dataset showed that various features such as "source," "destination," "protocol," "type," and "type of attack" have categorical values. The LabelEncoder from the sci-kit-learn library was used to address categorical variables in the dataset. "Label Encoding is a technique that involves transforming categorical variables into numerical data", enabling machine learning models that exclusively accept numerical inputs to process them effectively (Malik et al., 2024).

3.5.3 Data Standardization

Data standardization is another step in the data preprocessing phase in building machine models, which involves scaling numerical features to a common scale. This

process ensures that all features “have a mean of zero and a standard deviation of one” (Alghanmi, 2024), enabling them to be compared and facilitating the convergence of optimization algorithms during model training. Standardizing data prevents larger-scale variables from disproportionately influencing the learning process and dominating the results.

3.5.4 Stratified K-Fold Cross-Validation and Data Splitting

This section discusses dividing the dataset into multiple sets using Stratified K-Fold cross-validation. This technique is particularly useful for ensuring that each fold is a sizeable sample of the whole, especially in the case of imbalanced datasets.

3.5.4.1 Stratified Sampling

Stratified sampling ensures that the distribution of different classes is equally represented between the training and testing sets so that proper generalization occurs (Sharma, 2017). It is the most crucial step, especially for datasets with imbalanced classes. It retains the distribution of classes, hence making the model learn effectively and give better predictions across all different classes.

3.5.4.2 Stratified K-Fold Cross-Validation

In this praxis, the cross-validation (CV) techniques, including “the Stratified k-fold cross-validation, were employed in further validating the performance done by the model” (Bensaid et al., 2024). With Stratified “k-fold cross-validation, “the dataset is divided into k parts, each with a similar distribution of the target variable” (Prusty et al., 2022). This technique ensures one achieves a robust estimate of performance and, at the same time, avoids overfitting.

3.5.4.3 Data Splitting

In this praxis, the preprocessed dataset was divided in such a way that 80% of them belonged to the "training set, and the rest, 20%, were used for the test set" (Zahra et al., 2015). "The training set is used for optimizing the parameters of the model while the test set is considered as an independent set to locate the performance of the model" (Birchha & Nigam, 2022).

3.5.5 Balancing the Dataset

In this praxis, to address the class imbalance in the dataset, techniques such as "the Synthetic Minority Over-sampling Technique (SMOTE) were applied to generate synthetic samples for the minority class," particularly focusing on instances where the 'Type' column had values of 0 and 1 (Li, 2014). This approach balanced the dataset and ensured that the model did not become biased towards the majority class.

Additionally, under-sampling techniques were used to reduce the number of samples in the minority class, further balancing the dataset. For example, instances with a "Type" value of 0 were randomly sampled to match the count of instances with a "Type" value of 1. This step is performed in order to reduce the negative effect attributed eventually to the two categories, therefore boosting the performance of the machine learning models by obtaining an adequate and equilibrated distribution of both categories in the training data. Hence, this pre-processing step is considered a classifier, which is utilized to reduce the imbalance of the dataset applied in the machine learning techniques, thus producing more reasonable data that can be handled more efficiently in training and evaluating a machine learning model.

3.6 Building Machine Learning Models

This section discussed the model CNN-FL model development as well as the centralized DL models used for performance comparison. Section 3.6.1 describes the CNN-FL approach, while Section 3.6.2 describes the centralized deep learning models used to evaluate the performance of the proposed CNN-FL model.

3.6.1 CNN-Federated Learning Approach

The CNN-FL approach leverages the privacy-preserving benefits of federated learning while "utilizing the powerful feature extraction capabilities of Convolutional Neural Networks (CNNs)" (Cheng et al., 2017). This section provides additional insights into the CNN-FL model's architecture, training, and evaluation.

3.6.1.1 CNN Architecture

The CNN architecture used in this praxis "comprises of various layers, such as convolutional layers, pooling layers, and fully connected layers" (Ghourabi et al., 2024). The "convolutional layers are designed for extracting spatial features from the input data" (Al-Hadhrami et al., 2024), using filters to detect patterns and edges, whereas "the pooling layers diminish the spatial dimensions of the feature maps, enhancing the computational efficiency and minimizing the risk of overfitting" (Ntizikira et al., 2023). On the other hand, "the fully connected layers combine the extracted features to make predictions" (Le et al., 2024). The final "layer uses a sigmoid activation function for binary classification or a softmax activation function for multi-class classification" (Banerjee, 2023).

3.6.1.2 Federated Learning Process

The federated learning process involves multiple rounds of training between the central server and the clients, with each round consisting of the following steps as detailed below (Gafni et al., 2022):

a) **Model Initialization**: "The central server initializes the global CNN model "with random weights and sends it to all participating clients (Zhang et al., 2023).

b) **Local Training**: Clients use their local data to train the model for a fixed number of epochs. Each client updates the model weights based on its local dataset.

c) **Model Aggregation**: Clients send their updated model weights to the central server, where they are aggregated using the weighted Federated Averaging (FedAvg) algorithm. This algorithm computes a weighted average of the updates, with weights proportional to the number of data samples on each client.

d) **Global Model Update**: The aggregated model is updated and sent back to the clients for the next round of training.

3.6.1.3 Federated Learning Aggregation

Federated learning aggregation techniques are essential for decentralized machine learning systems, particularly in sensitive privacy contexts like intrusion detection. These strategies determine how local updates from individual devices or clients are combined to form a global model without breaching data privacy. Although several aggregation methods are available, such as weighted federated average (weighted FedAvg), federated proximal (FedProx), and federated stochastic gradient descent (FedSGD), weighted FedAvg is widely considered to be the best option for preserving privacy in machine learning intrusion detection models.

FedAvg is a seminal federated learning algorithm, which enables multiple clients to train a shared machine learning model in a collaborative manner without exchanging their local data (Eshan et al., 2023). In each iteration of the FedAvg process, clients conduct local training on their own data for several epochs and send the model parameters to a central server. Subsequently, "the central server aggregates these models (typically by averaging), to update the global model" (Tang et al., 2024).

FedProx is a variation of FedAvg in which a proximal "term is added to the objective function so that the local model can better mimic the global model" (Kaur et al., 2024). The proximal term in FedProx prevents the local model from deviating too much from the global model, with the purpose of improving model performance, especially in scenarios where clients' data distributions are highly heterogeneous.

FedSGD is another federated learning algorithm that extends the traditional stochastic gradient descent (SGD) optimization method to the federated setting in which, each client in a federated network performs local model training using its own data and computes model updates based on SGD. "These local updates are then aggregated at a central server to update the global model" (Si-Ahmed et al., 2024).

In weighted FedAvg, clients train models locally using their respective datasets and then share model updates with a central server, aggregating them by computing the weighted average to form a global model. This method effectively preserves privacy as it ensures that raw data samples remain on client devices, with only model updates being transmitted to the central server, minimizing the risk of data exposure. Additionally, the weighted FedAvg stands out as a widely utilized aggregation method in federated

learning, particularly valuable for privacy-preserving machine learning intrusion detection models (McMahan et al., 2017).

In this praxis, the weighted FedAvg aggregation method was used. The introduction of this federated learning aggregation method enhances the performance, privacy, and scalability of the CNN-FL model. Furthermore, by involving and incorporating this aggregation method, the proposed federated learning model can effectively address the challenges of decentralized machine learning models, particularly in sensitive privacy contexts like intrusion detection in healthcare environments.

3.6.1.4 Client Data Selection

The process of selecting clients to contribute their data for model training during each phase of a federated learning system is known as client data selection in FL (Alazab et al., 2023). The choice of clients for model training has an immediate impact on the global model's representation and its generalization performance on unseen data. Random selection, stratified selection, proactive selection, and dynamic selection are several widely used client selection strategies in FL (Alazab et al., 2023).

In random selection, clients are selected randomly during each iteration. This section method ensures that all clients are equally likely to be chosen. On the other hand, the proactive client selection technique strives to anticipate how much the clients can contribute to the global model's quality based on their data characteristics and past performance analysis. Its objective is to prioritize the clients whose data “is expected to contribute the most to the global model's accuracy and robustness” (Alazab et al., 2023).

In contrast to the random and proactive client selections, the dynamic client selection method adjusts the process of selecting clients with respect to the feedback

received from the clients during the course of training. It keeps evaluating the performance of the clients' contributions continuously during the training and dynamically selects the clients that can help improve the learning process, which enforces the model's adaptation to changes in the data distribution and client availabilities (Alazab et al., 2023).

In stratified selection, clients are chosen based on the characteristics of their local data such as data size and the data distribution. More specifically, "the clients with larger data sizes or more representative data distributions" will be more likely to be selected (Alazab et al., 2023). The purpose of this methodology is to select the clients that are more representative and can make more valuable contributions to the global model.

In this praxis, stratified selection was used. This method enables a good representation of the whole dataset and avoids overrepresenting a single cluster of clients. Thus, the global model can generalize well to unseen data, providing a more stable and reliable performance than proactive and dynamic methods.

3.6.1.5 CNN-FL model architecture

The federated learning model architecture is implemented using TensorFlow Federated (TFF), a federated learning platform (Aledhari et al., 2020). The model is defined as a sequential neural network with the following layers:

- Input Layer: Input shape is set to (5), indicating a 1D tensor with 5 features.
- Dense Layers: Three dense layers with 64, 64, and 32 neurons, respectively.
- Activation Function: Rectified Linear Unit (ReLU) is used to promote non-linearity and feature extraction (Aljameel, 2022).

- Output Layer: A final dense layer with a single neuron, utilizing a sigmoid activation function. This configuration is suitable for binary classification tasks (Verma et al., 2022).

The model includes metrics like accuracy, precision, and recall for evaluation and uses a “binary cross-entropy for binary classification and sparse categorical cross-entropy for multi-class classification as a loss function” (Lakshmanamoorthy, 2021). The server optimizer uses the Adam optimizer with a higher learning rate of 0.05, while the client optimizer uses the Adam optimizer with a lower learning rate of 0.0.1. This ensures a federated averaging mechanism that adjusts the global model based on aggregated updates from participating clients.

3.6.2 Centralized Deep Learning Models

To assess the CNN-FL's performance, it is compared with three centralized deep learning (DL) models: Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), and Deep Neural Network (DNN).

3.6.2.1 CNN

Convolutional Neural Network (CNN) is defined using TensorFlow's Sequential model API, tailored for a binary classification task. The network architecture includes a convolutional layer ‘Conv1D’ with 32 filters and a kernel size of 3, followed by a dropout layer to prevent overfitting. After flattening the convolutional layer's output, a dense layer with a sigmoid activation function is used to make the binary prediction. The model is compiled with the Adam optimizer with a learning rate of 0.01, “binary cross-entropy for binary classification, and sparse categorical cross-entropy for multi-class classification as the loss function” (Lakshmanamoorthy, 2021). Accuracy is used as the

performance metric. Training is performed over 100 epochs with a batch size of 20 and includes validation with ‘X_test’ and ‘y_test’.

3.6.2.2 DNN

The DNN architecture “consists of an input layer with 5 neurons and three densely connected layers with 32, 64, and 32 neurons, respectively with each layer activated by the rectified linear unit (ReLU) function” (UrRehman et al., 2024). The final layer is a dense layer with neurons equal to the number of classes, employing a softmax activation function for multiclass classification. Similar to the previous models, the DNN neural network is “compiled using the Adam optimizer with a learning rate of 0.01, “binary cross-entropy for binary classification, and sparse categorical cross-entropy loss” (Lakshmanamoorthy, 2021). The training process spans 100 epochs with a batch size of 20, and model performance is monitored on the validation data.

3.6.2.3 RNN

The RNN model is designed for multiclass classification. It comprises a single SimpleRNN layer with 32 units, followed by a Dropout layer with a dropout rate of 0.5 to prevent overfitting. “The output layer is a Dense layer with a softmax activation function, suitable for handling multiclass classification tasks” (UrRehman et al., 2024). The model is compiled using the Adam optimizer with a learning rate of 0.01, binary cross-entropy for binary classification, and sparse categorical cross-entropy loss for multi-class classification. Training is conducted for 100 epochs, with a batch size of 20, and model performance is evaluated on the provided validation data. Confusion matrix, accuracy score, and a detailed classification report are generated to assess the model's classification

performance. Additionally, training, prediction, and the total process time are recorded for comprehensive evaluation.

3.7 Model Evaluation

The proposed model's performance evaluation relies on several parameters, including accuracy, precision, recall, F1-Score, and false alarm rate, rounded to binary values. This praxis also considered the four metrics of "the confusion matrix to evaluate the performance of the classification model, namely the "true positive (TP)," the "false positive (FP)," the "true negative (TN)," and the "false negative (FN)," which are defined as follows" (Bhavsar et al., 2023):

- TP: "All instances of any class that are classified as the correct class" (Bhavsar et al., 2023).
- FP: "All the non-instances of any class that are classified as the correct class" (Bhavsar et al., 2023).
- TN: "All the non-instances of class that are not classified as the correct class" (Bhavsar et al., 2023).
- FN: "All instances of a particular class that are not classified as correct" (Bhavsar et al., 2023).

"Accuracy is estimated as the ratio of accurately classified records to the total number of records or counts" (Mehdary et al., 2024), as in Equation 3.1 below:

$$Accuracy = \frac{\boldsymbol{TP+TN}}{\boldsymbol{TP+TN+FP+FN}}$$

Equation 3-1: Accuracy

"Precision calculates the ratio of correctly predicted positive outcomes to the total predicted positives" (Mehdary et al., 2024), as given in Equation 3.2:

$$Precision = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FP}}$$

Equation 3-1: Precision

"Recall computes the ratio of correctly predicted positive outcomes to all outcomes in a specific class" (Mehdary et al., 2024), as given in Equation 3.3:

$$Recall = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FN}}$$

Equation 3-2: Recall

"F1 Score is a combined metric of precision and recall" (Seung-Jun, 2020), ranging from 0 to 1as given in Equation 3.4:

$$F1\text{-}Score = \mathbf{2}\frac{\boldsymbol{Precision*Recall}}{\boldsymbol{Precison+Recall}}$$

Equation 3-3: F1-Score

"False Alarm Rate (FAR) represents the probability of falsely declaring the presence of a condition or event when it is not actually present" (Seung-Jun, 2020), as given in Equation 3.5:

$$\text{FAR} = \frac{\boldsymbol{FP}}{\boldsymbol{FP+TN}}$$

Equation 3-4: False Alarm Rate

Chapter 4—Results

4.1 Introduction

This praxis aims to enhance security and privacy in healthcare organizations by building a Convolutional Neural Network (CNN)-Federated Learning (FL)-based Intrusion Detection System (IDS) that can detect and classify cyber threats to the Internet of Healthcare Things (IoHT) devices. The goal of this chapter is to analyze the proposed model's performance in detecting and classifying cyber threats while maintaining the privacy of patient data.

After the opening introduction, section 4.2 briefly describes the ECU-IoHT dataset. Section 4.3 presents the results of the exploratory data analysis (EDA) carried out in this praxis. Section 4.4 then presents the results of the various data preprocessing steps that were taken to prepare the ECU-IoHT dataset for the CNN-FL model tested in this praxis. Section 4.5 and its subsections present the results of the CNN-FL binary and multi-class classification models. Finally, section 4.6 concludes this Chapter with the results of the centralized deep-learning models that are used to evaluate the performance of the proposed CNN-FL intrusion detection model.

4.2 Description of the ECU-IoHT Dataset

The ECU-IoHT dataset was created to help the healthcare security professional analyze cyberattacks on IoHT in an IoHT environment. The dataset was generated through a simulated IoHT network that contained various medical sensors, which were subjected to different types of attacks. Figure 4-1 provides some basic statistics on the dataset, which contains 23453 instances of normal activities and 87754 instances of

attacks. Table 4-1 further summarizes the attack distribution across 4 categories: Smurf Attack, Nmap Port Scan, ARP Spoofing, and DoS Attack.

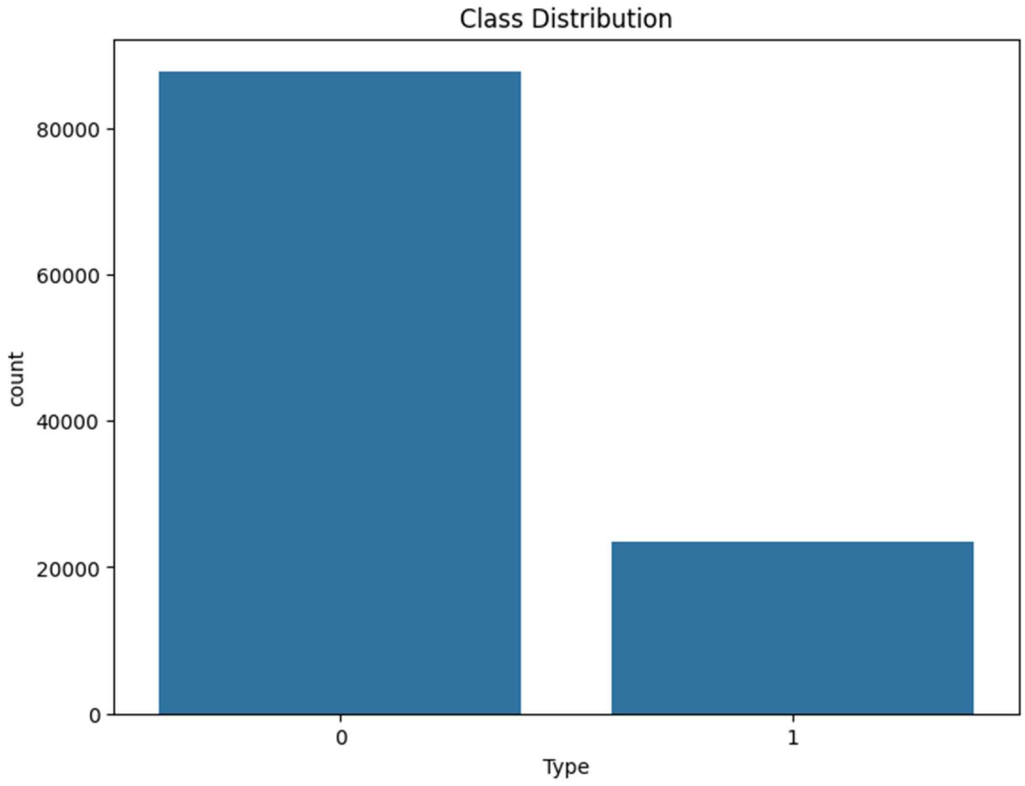

Figure 4-1: Distribution of the Target Feature "Type"

Table 4-1: Count of "Type of Attack"

Type of attack	Value count
Smurf attack	77920
Nmap Port Scan	6836
ARP Spoofing	2359
DoS attack	639

4.3 Exploratory Data Analysis

The ECU-IoHT dataset was examined comprehensively during the EDA section to uncover patterns, trends, and insights. Through statistical summaries, visualizations, and data exploration techniques, a deeper analysis of the dataset's underlying structure and characteristics is performed, which lays the foundation for informed decision-making and subsequent modeling efforts.

Table 4-2 below presents the results of various statistical metrics of the ECU-IoHT dataset features using the describe () function, which generates “the count, mean, standard deviation, minimum and maximum values, and the quantiles” of the dataset (Patil, 2022). It can be observed from the result depicted in this table that the features in this dataset have different scales, as evidenced by the differences in means and standard deviations among the features. For instance, the mean value for the 'Time' feature is 6117.07, the median value is 7311.92, and the standard deviation is 2337.34 for the “Time” feature. On the other hand, the minimum value is 0.00, and the maximum value is 10109.39. Contrarily, the 'Length' feature has different values: the mean is equal to 112.66, and the standard deviation is equal to 287.89. However, the minimum, the maximum, and the first quartile are all equal to 42.00. These observations suggest that the data points are spread out from the mean, providing insights into the distribution shape and enabling the identification of potential outliers. Normalization or standardization techniques can be applied to rescale the features to a similar range to ensure that features with larger magnitudes do not dominate the model's learning process.

Table 4-2: Summary Statistics for ECU-IoHT Dataset Feature

	No.	Time	Length
Count	**111207**	**111207**	**111207**
Mean	**55604**	**6117.08**	**112.66**
Std	**32102.84**	**2337.34**	**287.89**
Min	**1**	**0**	**42**
Max	**27802.50**	**6178.69**	**42**
25%	**55604**	**6745.55**	**42**
50%	**83405.50**	**7311.923**	**54**
75%	**111207**	**10109.39**	**1474**
Max	**111207**	**111207**	**111207**

Next, this praxis examined the dataset columns to determine their corresponding data types using the info () function. As shown in Table 4-3, this dataset comprises nine features classified into three distinct data types: int64, float64, and object. Among these, two features are of int64 type, one is of float64 type, and six are of the object type. As previously discussed in the Chapter above, the machine learning techniques used in this praxis can only process numerical data. Therefore, the int64 and float64 features are suitable, while the object data type features must be mapped to numerical values to enable the ML models to process them.

Table 4-3: Dataset Features and Types

Features	Data Types
No.	int64
Time	float64
Source	object
Destination	object
Protocol	object
Length	Int64
Info	object
Type	object
Type of attack	object

Furthermore, it can be observed that null/missing values do not exist in the ECU-IoHT dataset as the result shown in Table 4-4.

Table 4-4: Count of NA Values in the Dataset

Features	Counts of N/A
No	0
Source	0
Destination	0
Protocol	0
Length	0
Info	0
Type	0
Type of attack	0

In addition to the summary statistical analysis, the distribution of each feature was analyzed to understand their underlying patterns. Histograms and boxplots were utilized to visualize the distributions, as illustrated in Figure 4-2 and Figure 4-3 below. For example, the “Length” feature exhibited a right-skewed distribution, indicating a concentration of shorter lengths with a few exceptionally long instances.

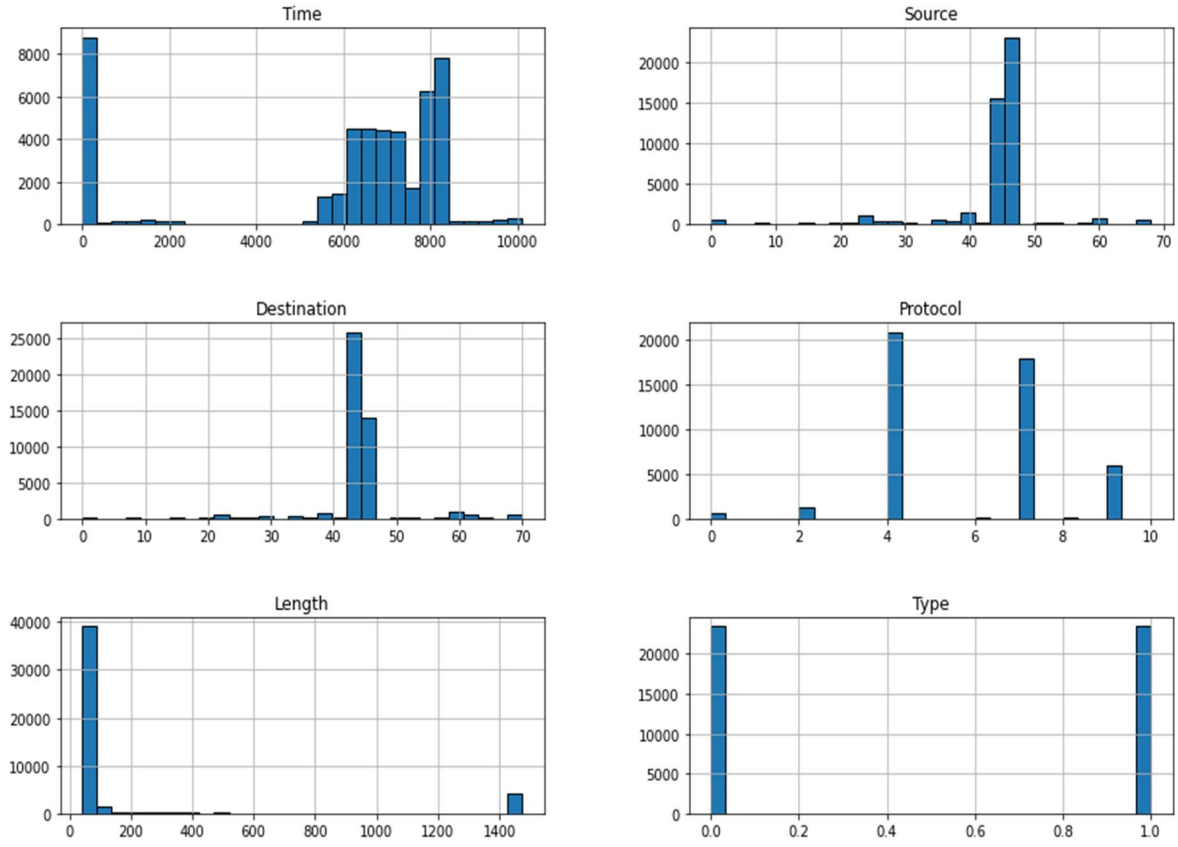

Figure 4-2: Distribution of Individual Features of the Dataset

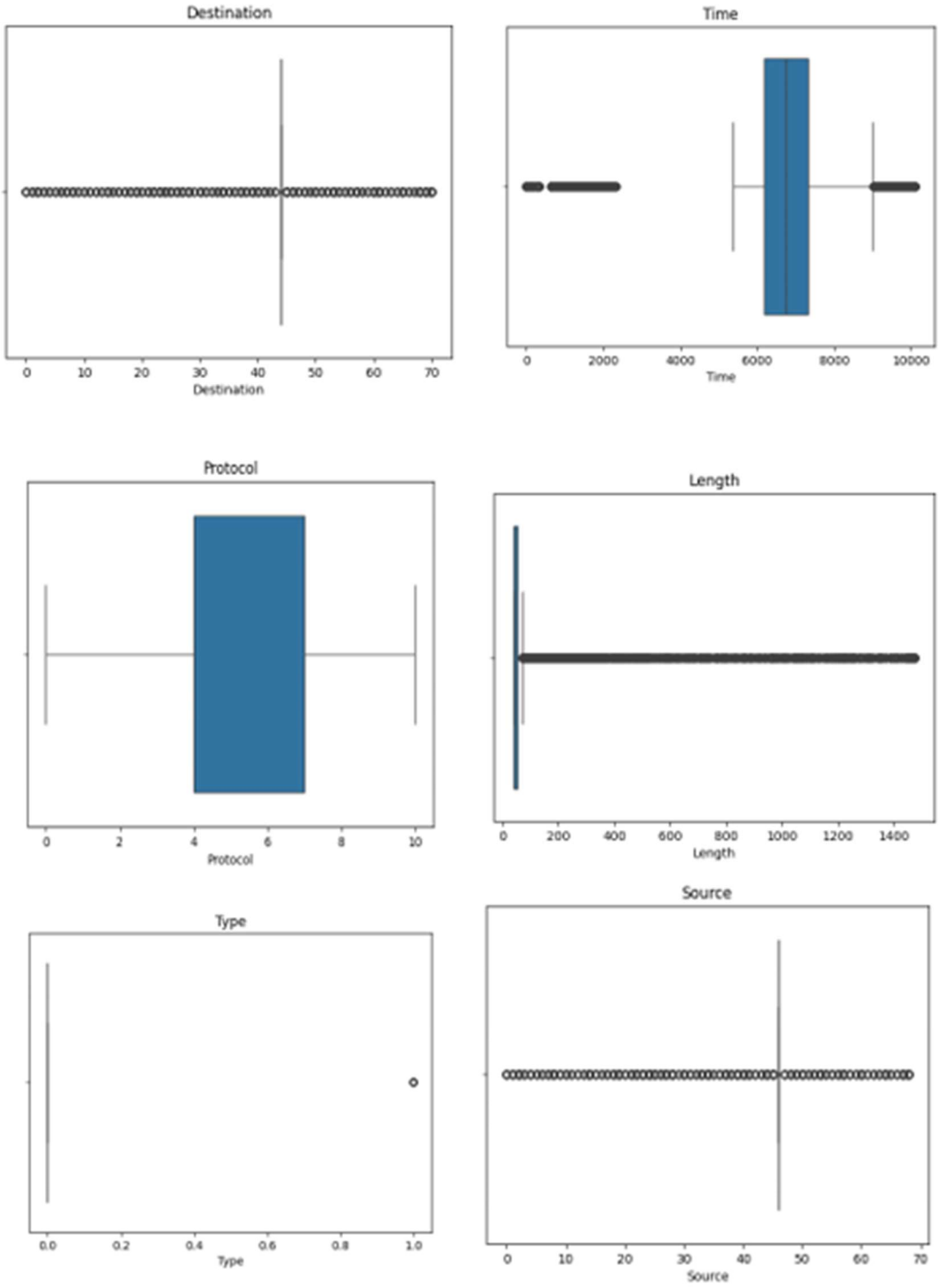

Figure 4-3: Boxplot of Individual Features of the Dataset

Moreover, in this praxis, the correlation heatmap was plotted to show how dependent the features are on one another. Figures 4-4 below show the correlation matrix is symmetric and has a diagonal of 1s, indicating a perfect correlation between each variable and itself. Darker shades of brown and purple represent stronger positive or negative relationships, while lighter shades indicate weaker connections.

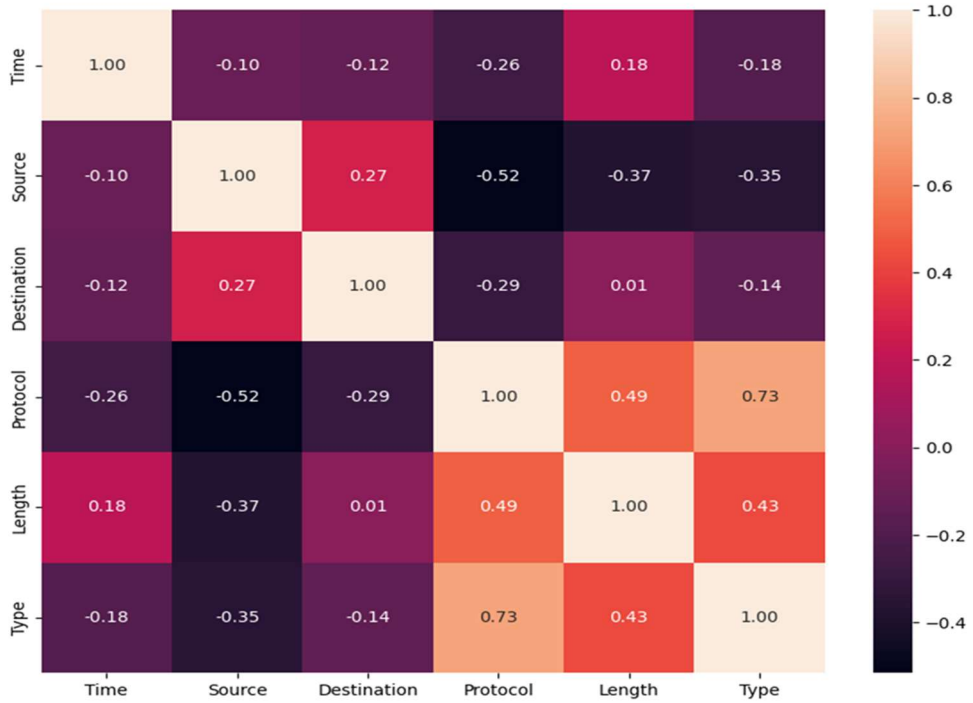

Figure 4-4: Correlation Heatmap of the ECU-IoHT Dataset Features

Notable observations in the matrix include a moderate negative correlation between Time and Protocol (-0.26), which suggests that higher Protocol values are associated with lower Time values. Moreover, Protocol and Type show a strong positive correlation (0.73), indicating simultaneous increases. The Source variable demonstrates a moderate negative correlation with Protocol and Type (-0.52 and -0.35, respectively), indicating that higher Source values tend to coincide with lower Protocol and Type

values. On the other hand, “Destination” exhibits minimal to no correlation with other variables, suggesting independence in terms of linear relationships.

Beyond correlation, this praxis also plotted scatter plots in Figure 4-5 to visualize the pairwise relationships between numerical features. These plots help in identifying non-linear relationships and interactions that could be missed by simple correlation coefficients. For example, while “Time” and “Length” had a weak correlation, the scatter plot indicated a clustered pattern, suggesting potential subgroups within the data that could be relevant for clustering or classification tasks.

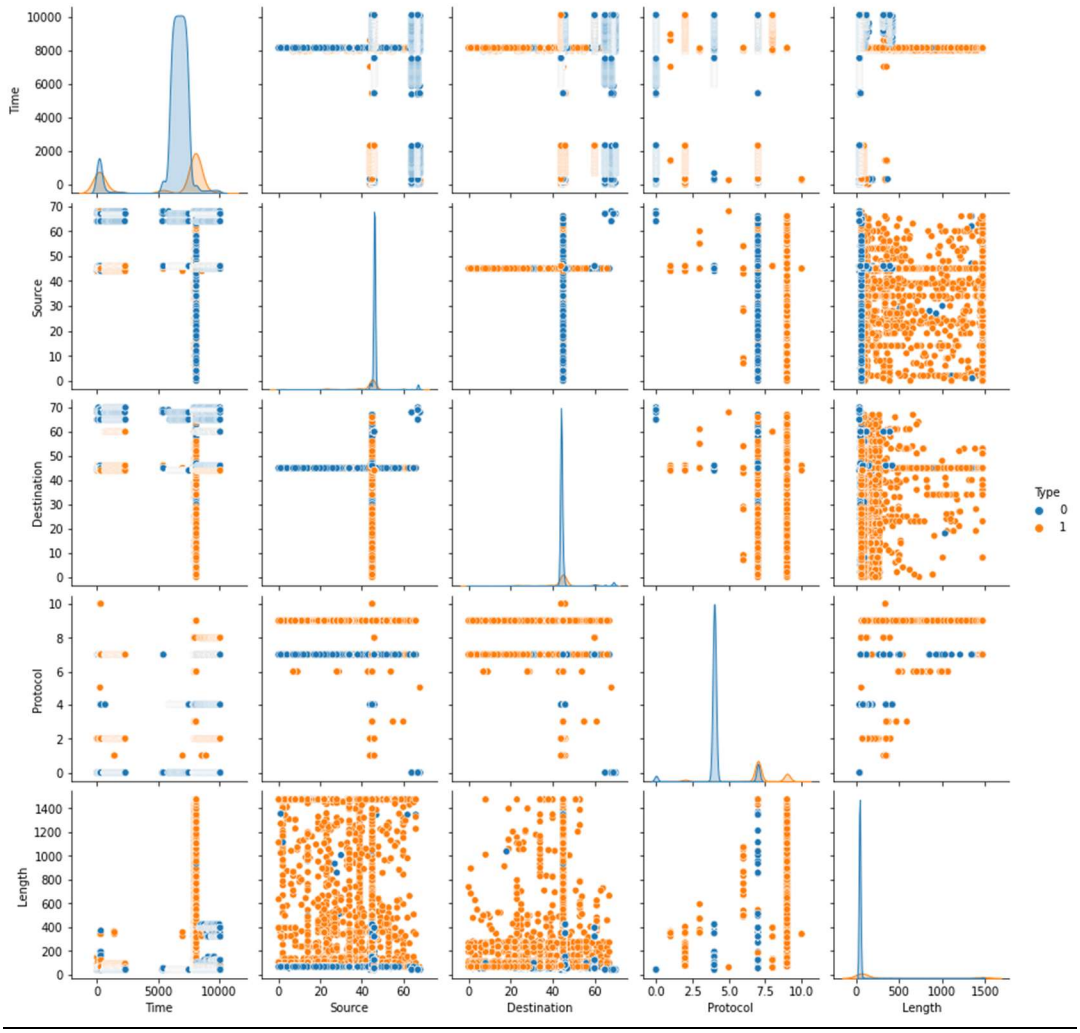

Figure 4-5: Scatter Plots of the ECU-IoHT Dataset Features

4.4 Federated Learning Aggregation Method Selection

As discussed in Chapter 3, the federated aggregation used in the federated model (FL) model is crucial in federated learning models, as it plays a central role in aggregating and combining the locally trained model updates from different client devices or nodes without compromising data privacy. In this praxis, the following FL aggregation methods such as weighted federated average (weighted FedAvg), federated

proximal (FedProx), and federated stochastic gradient descent (FedSGD), were evaluated to determine the FL aggregation that will yield a higher model accuracy. Table 4-5 describes the performance results of each FL aggregation method. For simplicity, this evaluation is limited to the FL multi-class classification for 15 clients.

Table 4-5: Performance Results for FL Aggregation Methods

	Accuracy	Precision	Recall	F1-score	FAR
FedSGD	0.9262	0.9037	0.8920	0.8891	0.0171
FedProx	0.9542	0.9335	0.9338	0.9336	0.0106
Weighted FedAvg	0.9743	0.9637	0.9630	0.9629	0.0050

The result notes that weighted FedAvg helps the proposed model achieve a higher performance rate compared to the FedSGD and FedProx aggregation methods.

4.5 Model Evaluations

The section below presents the performance evaluation of the Convolutional Neural Network (CNN)-Federated Learning (ML)-based intrusion detection model to detect and classify cyber threats on IoHT devices. The primary measures of interest are accuracy (acc) and false alarm rate (FAR). This praxis also considers the precision, the recall, and the F1 score. Moreover, this praxis considers both binary and multi-class classification for 15, 10, and 5 clients.

4.5.1 CNN-FL for the Binary Classification Approach

Table 4-6 presents the results of the CNN-FL model using the ECU-IoHT dataset. The model exhibits an accuracy score of 99.20%, 99.04%, and 98.99% for the 15, 10, and 5 clients, respectively. This demonstrates that the model possesses a high degree of

reliability in predicting positive classes and distinguishing them from negative classes. Additionally, the precision, recall, and f1 scores are higher than 98.00% across all clients' sizes, showing the model is stable for detecting cyber threats.

Regarding the FAR, the model with 15 clients has the lowest value of 1.42%. The other FAR values range from 1.88% to 1.99%, which demonstrates that the proposed model can improve the accuracy of cyber-attack detection.

Table 4-6: CNN-FL Binary Classification Results Summary for 15, 10, and 5 clients

Model/Clients	Accuracy	Precision	Recall	F1 score	FAR
CNN-FL (15 clients)	0.9920	0.9845	0.9988	0.9916	0.0142
CNN-FL (10 clients)	0.9904	0.9825	0.9995	0.9910	0.0198
CNN-FL (5 clients)	0.9899	0.9824	0.9983	0.9903	0.0188

4.5.2. CNN-FL for the Multi-Class Classification Approach

The results depicted in Table 4-7 show that the proposed solution achieves an accurate score of 97.43%, 97.60%, and 97.41% for 15, 10, and 5 clients, respectively. This is very indicative of an excellent classification performance. Additionally, the precision, recall, and f1 scores are higher than 96.00% across all clients' sizes, showing the model is stable for detecting cyber threats.

Regarding the FAR, the model with 10 clients has the lowest value of 0.55%. The other FAR is at 0.59%, which again demonstrates that the proposed model can be employed to improve the accuracy of cyber-attack classification.

Table 4-7: CNN-FL Multi-Class Classification Results Summary for 15, 10, and 5 Clients

Model/Client	Accuracy	Precision	Recall	F1 score	FAR
CNN-FL (15 clients)	0.9743	0.9637	0.9630	0.9629	0.0059
CNN-FL (10 clients)	0.9760	0.9663	0.9652	0.9653	0.0055
CNN-FL (5 clients)	0.9741	0.9637	0.9628	0.9625	0.0059

4.5.3 Centralized Deep-Learning (DL) Models

In this praxis, the proposed CNN-FL model is compared with centralized deep-learning models such as CNN, Deep Neural Network (DNN), and Recurrent Neural Network (RNN) to determine its efficacy. This section discusses the results of such models.

4.5.3.1 CNN Binary Classification

In Table 4-8, the CNN model demonstrates a high accuracy rate of 95.41% and an exceptional precision rate of 100.00% in distinguishing between normal and anomalous instances. Its high recall values in the range of 91.00% and 100.00% signify the effective identification of both normal and anomalous instances. The model's F1-Score of 96.00% suggests a robust performance in terms of both precision and recall, making it suitable for reliable anomaly detection. The CNN model showcases strong predictive capabilities and is well-suited for the task of anomaly detection in the given dataset.

Table 4-9 presents the results of the model training time as well as testing time. In terms of timing, the model has a considerable training time of over eight (8) minutes, and an impressive test time of less than one (1) second, which indicates the model can make

quick predictions after the initial investment in training. Overall, the model's metrics and confusion matrix depicted in Figure 4-6 suggest it is robust and well-suited for practical applications where high accuracy for a CNN binary classification.

Table 4-8: CNN Binary Classification Results Summary

	Precision	Recall	F1-score	Support
0	1.00	0.92	0.96	4625
1	0.92	1	0.96	4757
Accuracy			0.96	9382
Macro avg	0.96	0.96	0.96	9382
Weighted avg	0.96	0.96	0.96	9382

Table 4-9: Training Details for CNN Binary Classification

Timing Details	Time (seconds)
Training Time	531.91 seconds
Testing Time	0.70 seconds
Total Time	532.61 seconds

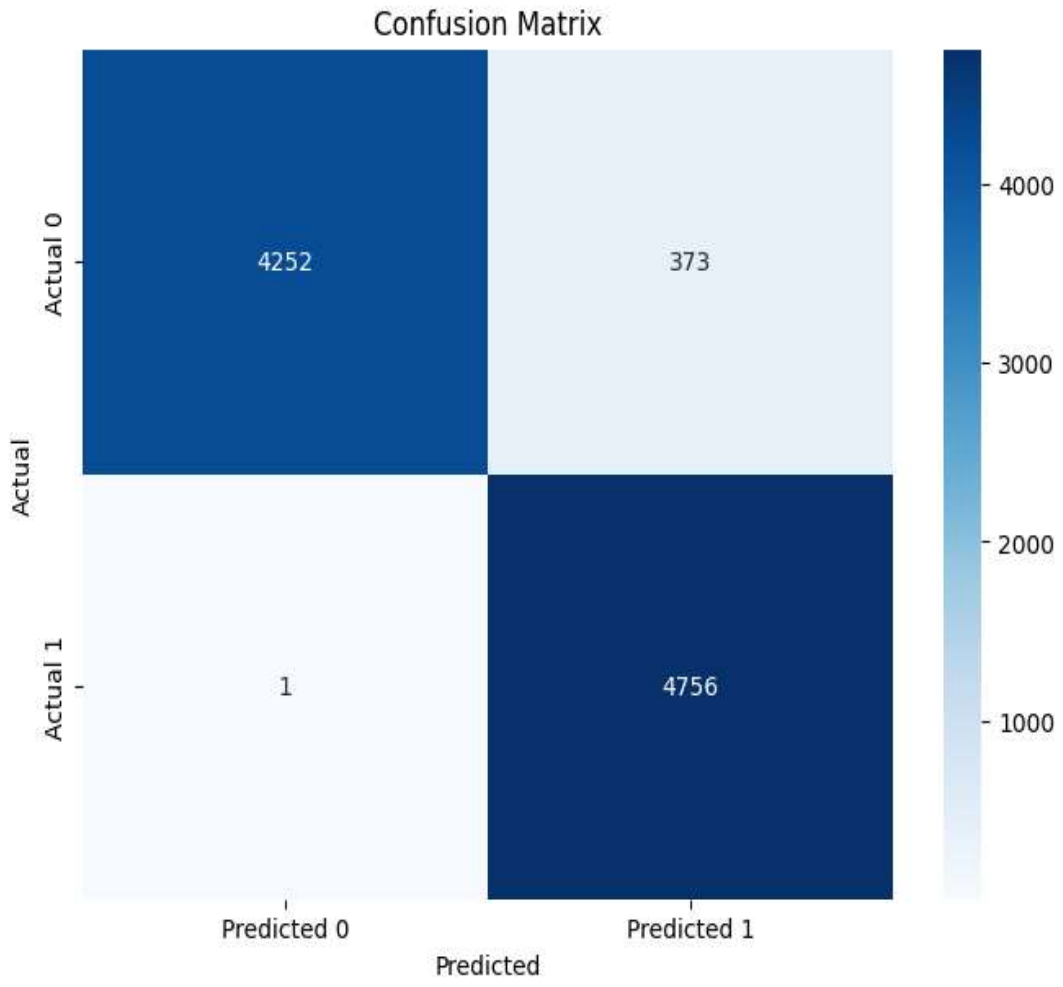

Figure 4-6: CNN for Binary Classification Confusion Matrix

4.5.3.2. RNN Binary Classification

In Table 4-10, the RNN model shows an accuracy rate of 99.25% and an exceptional precision rate of 100% in identifying normal instances from anomalous instances. Its high recall values signify the effective identification of both normal and anomalous instances. The model's balanced F1-Score suggests a robust performance in terms of both precision and recall, making it suitable for reliable anomaly detection.

Table 4-10: RNN Binary Classification Summary

	Precision	Recall	F1-score	Support
0	1.00	0.99	0.99	4625
1	0.99	1	0.99	4757
accuracy			0.99	9382
macro avg	0.99	0.99	0.99	9382
Weighted avg	0.99	0.99	0.99	9382

Table 4-11: Training Details for RNN for Binary Classification

Timing Details	Time (seconds)
Training Time	763.91 seconds
Testing Time	1.33 seconds
Total Time	765.24 seconds

In Table 4-11, the results of the model training time as well as testing time are presented. In terms of timing, the model has a considerable training time of over thirteen (13) minutes, and a relatively quick test time of a little over one (1) second, which indicates the model can make quick predictions after the initial investment in training. Additionally. model's metrics and confusion matrix depicted in Figure 4-7 suggest it is robust and well-suited for practical applications where high accuracy for a RNN binary classification.

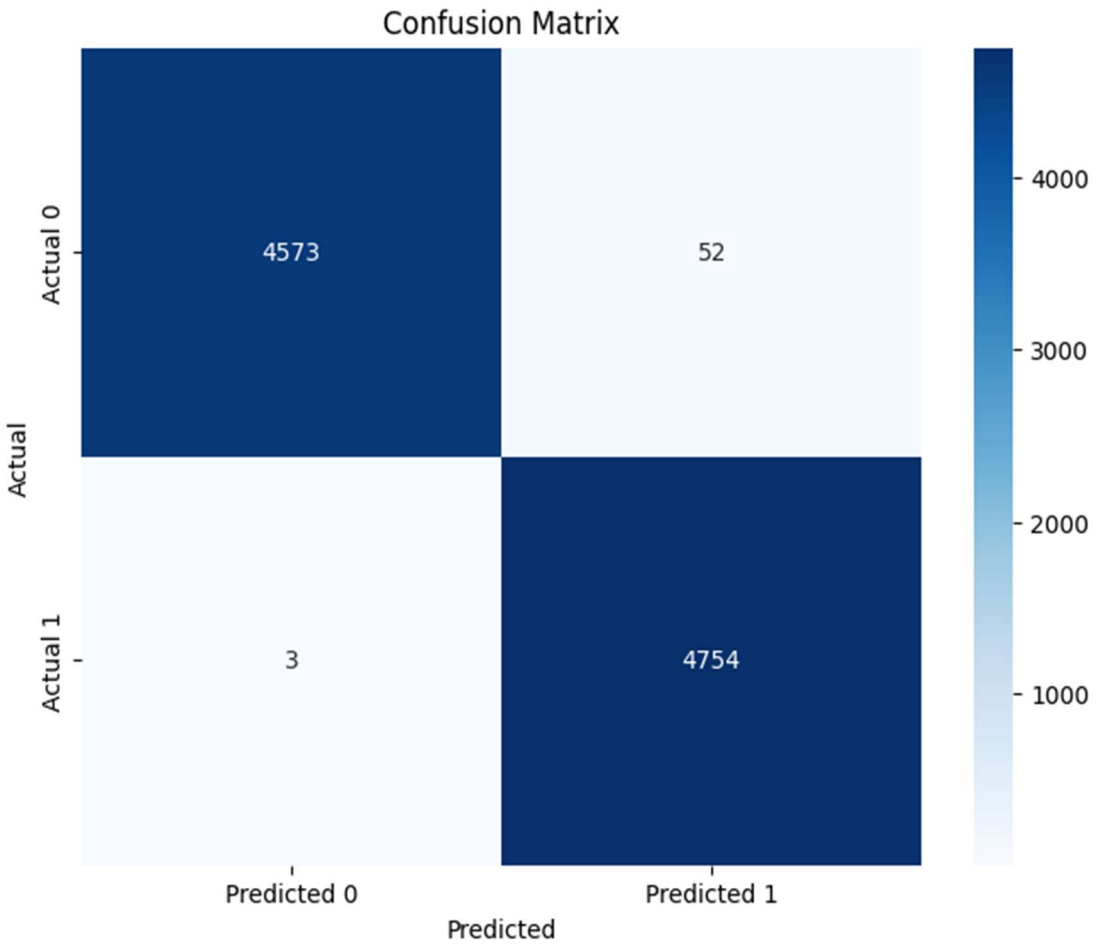

Figure 4-7: RNN for Binary Classification Confusion Matrix

4.5.3.3. DNN Binary Classification

The DNN model demonstrates a very good accuracy rate of 99% and precision rate of 100% in distinguishing between normal and anomalous instances. Its high recall values signify the effective identification of both normal and anomalous instances. The model's balanced F1-Score suggests a robust performance in terms of both precision and recall, making it suitable for reliable anomaly detection. The DNN model showcases strong predictive capabilities and is well-suited for the task of anomaly detection in the given dataset.

Table 4-12: DNN Binary Classification Result Summary

	Precision	Recall	F1-score	Support
0	1.00	0.99	0.99	4625
1	0.99	1	0.99	4757
accuracy			0.99	9382
macro avg	0.99	0.99	0.99	9382
Weighted avg	0.99	0.99	0.99	9382

Table 4-13: Timing Details for DNN Binary Classification

Timing Details	Time (seconds)
Training Time	291.15 seconds
Testing Time	0.658 seconds
Total Time	291.813 seconds

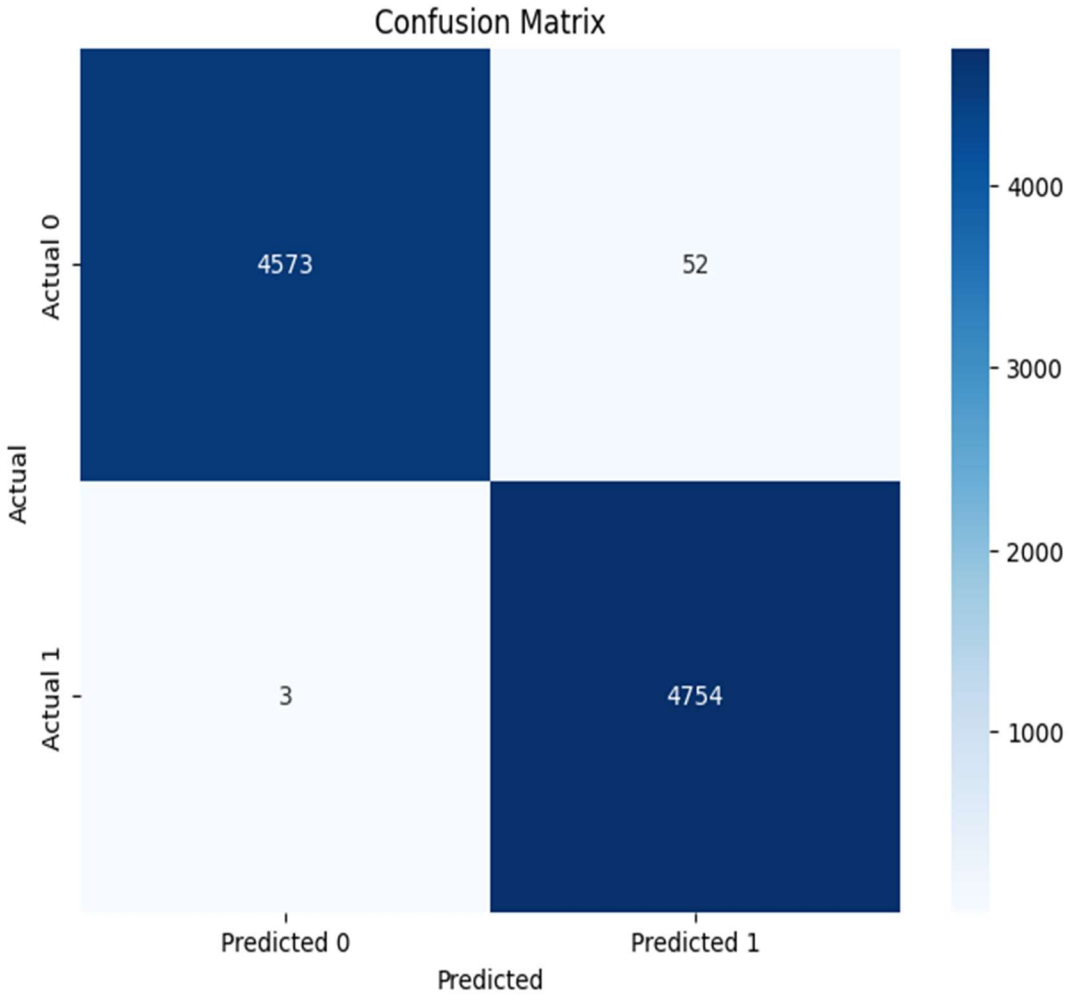

Figure 4-8: DNN for Binary Classification Confusion Matrix

As shown in Table 4-13, the model has a considerable training time of over four (4) minutes, and a relatively test time less than one (1) second, which indicates the model can make quick predictions after the initial investment in training. Additionally. model's metrics and confusion matrix depicted in Figure 4-8 suggest it is robust and well-suited for practical applications where high accuracy for a DNN binary classification.

4.5.3.4 CNN Multi-Class Classification

The CNN model displays a high level of accuracy in a multiclass classification context with an overall accuracy of 97.49%. Precision, recall, and F1-score are all consistently high across the classes, averaging between 96.00% and 97.00%, indicating a well-performing model across various metrics.

The confusion matrix reveals a high number of true positives along the diagonal, with Class 0 and Class 4 showing particularly strong performance. Some confusion is observed between Classes 2 and 3, as well as between Classes 1 and 2, suggesting these classes share similar features that the CNN is occasionally misinterpreting. In terms of timing, the model has a considerable training time of over 32 minutes, which is expected for CNNs dealing with complex patterns, especially in large datasets. The test time, however, is impressively brief, five (5) seconds, which means the model can make quick predictions after the initial investment in training. The total time is in line with the training duration, underscoring that the model's training phase is the most time-consuming part. Overall, the model's metrics and confusion matrix suggest it is robust and well-suited for practical applications where high accuracy in multiclass classification is required.

Table 4-24: CNN Multi-Class Classification Result Summary

	Precision	Recall	F1-score	Support
0	1.00	1.00	1.00	4790
1	0.95	0.95	0.95	4575
2	0.94	0.95	0.95	4575
3	0.90	0.89	0.90	4671
4	1.00	1.00	1.00	15598
accuracy			0.97	34347
macro avg	0.96	0.96	0.96	34347
Weighted avg	0.97	0.97	0.97	34347

Table 4-35: Timing Details for CNN Multi-Class Classification

Timing Details	Time (seconds)
Training Time	1948.08 seconds
Testing Time	5.18 seconds
Total Time	1953.26 seconds

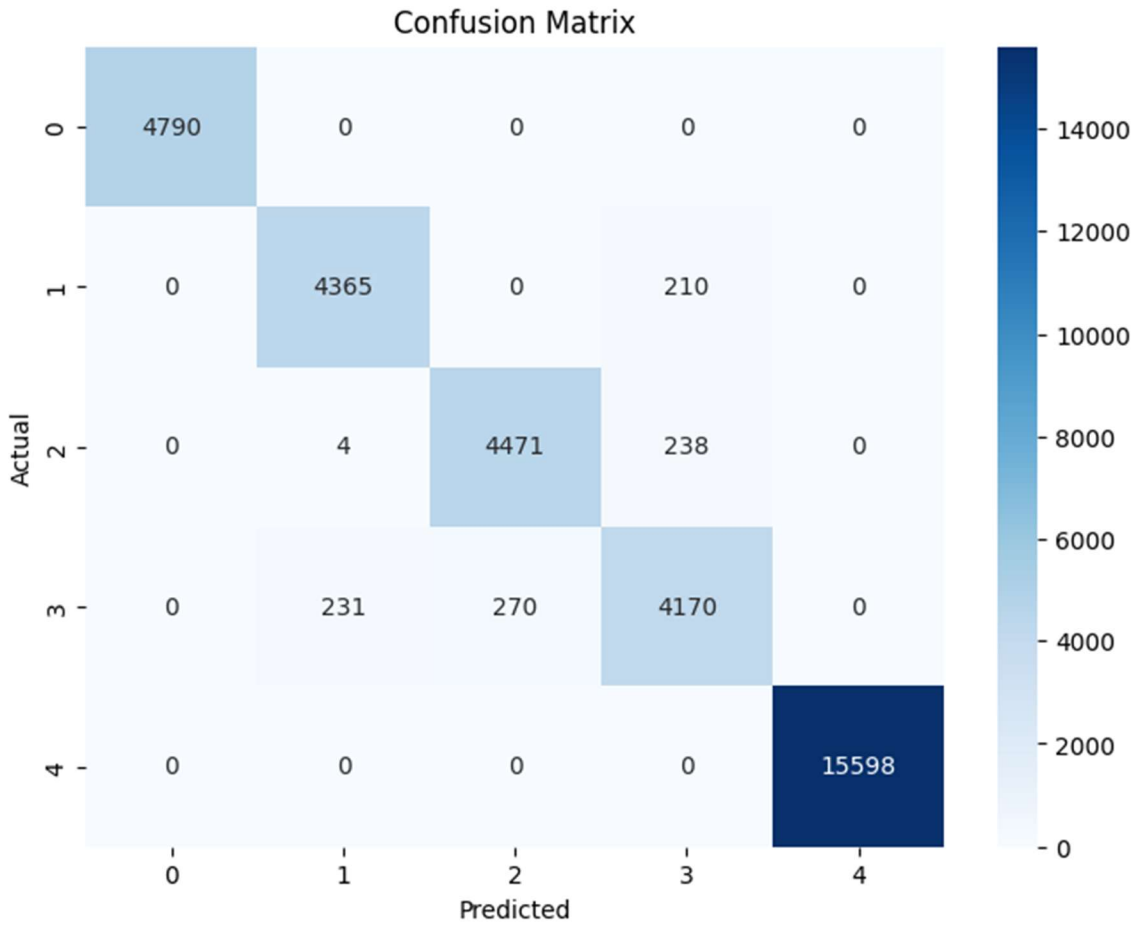

Figure 4-9: CNN Multi-Class Classification Confusion Matrix

4.5.3.5 RNN Multi-Class Classification

The RNN model has achieved high performance on a multiclass classification task, with precision, recall, and F1-scores all being high across the board, averaging 98.00%, which is indicative of a well-balanced model in terms of both precision and recall. Class 0 and Class 4 have perfect precision and recall scores, while the other classes also perform very well. The support values, which indicate the number of true instances for each class, show that the dataset is reasonably balanced, although Class 4 has significantly more instances. The overall accuracy of the model is 0.98, reinforcing its excellent performance. In terms of timing, the training time is substantial at just under

an hour, which is expected for RNN models that typically take longer to train due to their complex structures that process sequences. However, the test time is nearly 10 seconds, indicating the model's efficiency in making predictions once trained. The total time is just slightly more than the training time, suggesting that most of the time spent was for model training.

The confusion matrix provided complements the high-performance metrics previously mentioned. It shows that Class 0 and Class 4 were predicted with almost perfect accuracy, as evidenced by the high numbers on the diagonal and no misclassifications for Class 0. Class 1, 2, and 3 also show strong diagonal values, which means most instances were correctly classified. However, there are some instances of misclassification, as indicated by non-zero values off the diagonal. For example, Class 2 has been occasionally confused with Class 3, and similarly, Class 1 has been confused with Class 2 and Class 3. Despite these minor confusions, the model demonstrates a strong ability to distinguish between classes, which is particularly impressive given the larger number of instances in Class 4. The model's ability to accurately predict the majority class (Class 4) without significantly sacrificing the performance of minority classes suggests that it has effectively learned the distinguishing features of each class. This balance is crucial in multiclass classification problems, and the confusion matrix visually reinforces the model's robustness.

Table 4-46: RNN Multi-Class Classification Result Summary

	Precision	Recall	F1-score	Support
0	1.00	1.00	1.00	4790
1	0.92	0.98	0.95	4575
2	0.99	0.94	0.96	4513
3	0.94	0.93	0.94	4671
4	1.00	1.00	1.00	15598
accuracy			0.98	34347
macro avg	0.97	0.97	0.97	34347
Weighted avg	0.98	0.98	0.98	34347

Table 4-17: Timing Details for RNN Multi-Class Classification Result

Timing Details	Time (seconds)
Training Time	3544.47 seconds
Testing Time	10.41 seconds
Total Time	3554.88 seconds

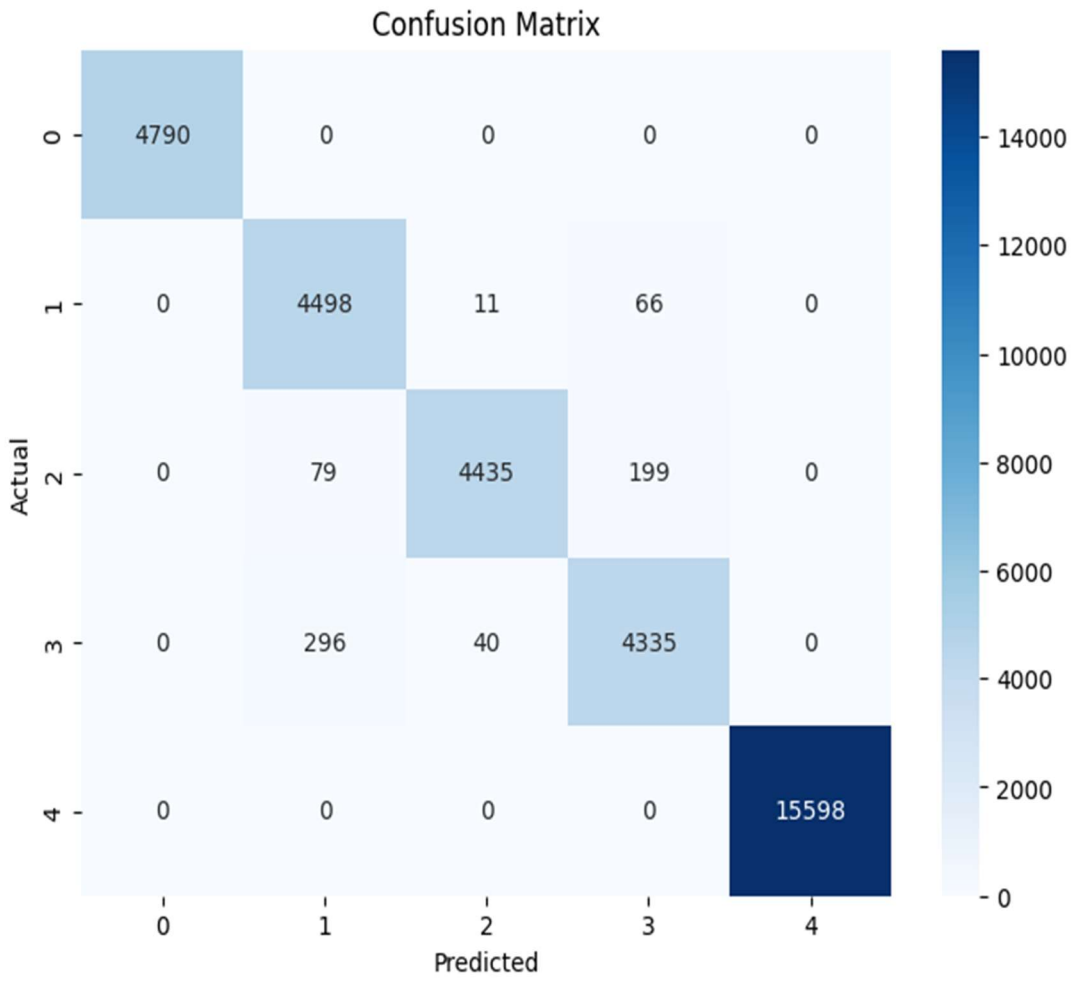

Figure 4-10: RNN Multi-Class Classification Confusion Matrix

4.5.3.6. DNN Multi-Class Classification

The DNN model's performance on a multiclass classification task is exceptional, with nearly perfect metrics: precision, recall, and F1-scores are all 99.00% on average, indicating a highly accurate and consistent model across all classes. The support values confirm a balanced dataset, with a significant number of instances for each class, particularly Class 4.

The overall accuracy of the model is 99.00%, which is outstanding and suggests that the model is well-tuned and generalizes the data very well. The confusion matrix visualizes this high performance, with most predictions concentrated on the diagonal,

indicating correct classifications. There are minimal misclassifications, which is a testament to the model's ability to distinguish between the classes effectively. The training time is lengthy, over 35 minutes, which is typical for complex DNN models that require extensive computation, especially on large datasets. However, the test time is nearly 7 seconds, suggesting that once trained, the model can make predictions quickly. The total time aligns closely with the training time, confirming the amount of time required in the training phase. This level of performance and efficiency in test time is indicative of a well-architected deep neural network.

Table 4-18: DNN Multi-class Classification Result Summary

	Precision	Recall	F1-score	Support
0	1.00	1.00	1.00	4790
1	0.96	1.00	0.98	4575
2	0.99	0.95	0.97	4575
3	0.95	0.95	0.95	4671
4	1.00	1.00	1.00	15598
accuracy			0.99	34347
macro avg	0.98	0.98	0.98	34347
Weighted avg	0.99	0.99	0.99	34347

Table 4-19: Timing Details for DNN Multi-class Classification

Timing Details	Time (seconds)
Training Time	1517.65 seconds
Testing Time	6.95 seconds
Total Time	1524.61 seconds

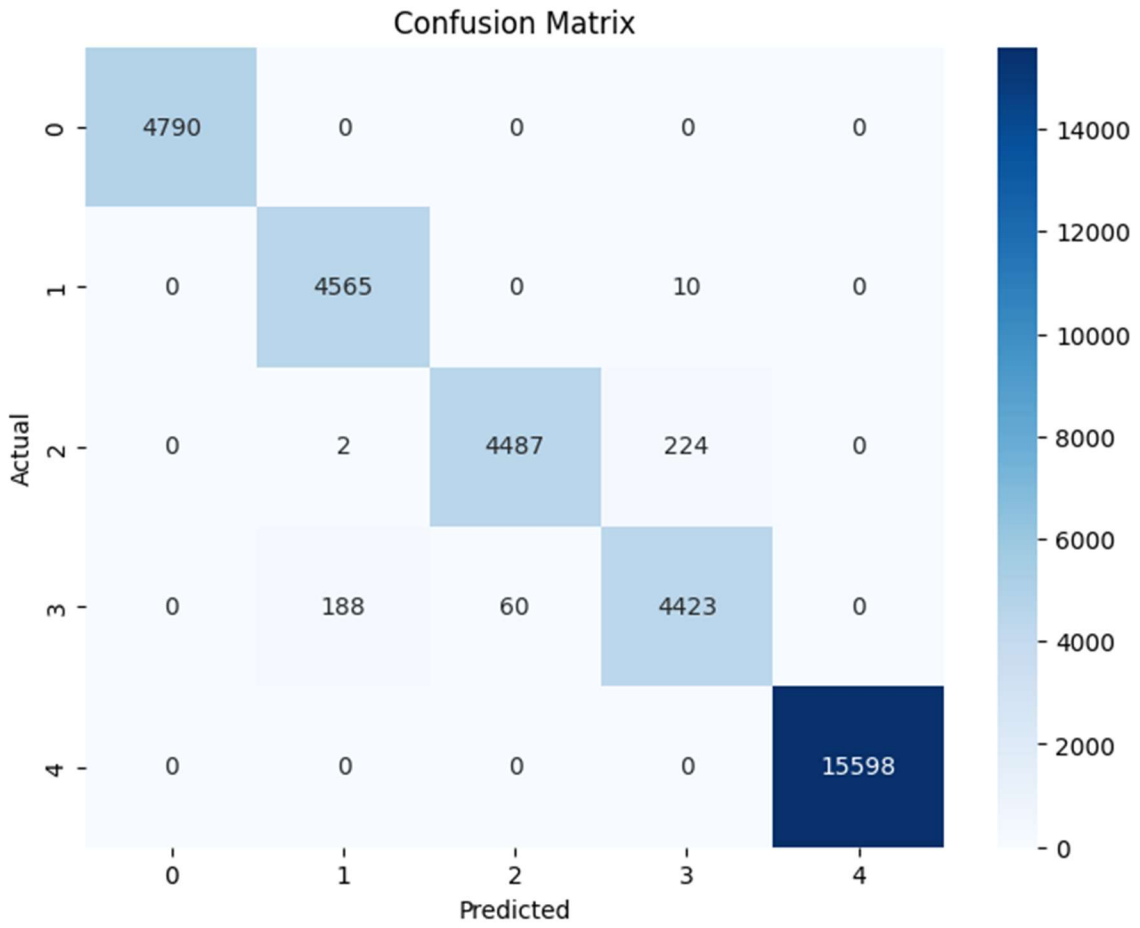

Figure 4-11: DNN Multi-class Classification Confusion Matrix

4.6 Model Comparison and Analysis

Comparing the CNN-Federated Learning (CNN-FL) model to deep learning models like CNN, DNN, and RNN, which are commonly deployed in a centralized

manner, yields several critical observations. Firstly, when compared against its centralized counterparts — CNN, DNN, and RNN — CNN-FL consistently, and significantly, performs almost at the same levels in terms of accuracy, precision, recall, and F1 score. Secondly, CNN-FL also consistently, and significantly, achieves lower false alarm rate (FAR), compared to CNN, DNN, and RNN. These results underscore the effectiveness of FL-based approach in advancing IoT based cyber-threats detection in healthcare networks.

One remarkable finding is the model's ability to handle non-identical independent identically distributed (NIID) data distributions across different clients. Traditional centralized models often face challenges due to variations in data distribution, resulting in degraded performance. In contrast, the federated learning scheme, especially with the adoption of the weighted FedAvg aggregation, exhibits robustness in aggregating diverse local updates to construct a coherent and accurate global model. This capability is essential in the IoHT scenario since data collected from various devices and environments can be highly heterogeneous.

4.7 Implications for Healthcare IoT Security

The results of this research are important for the adoption of cybersecurity strategies inside healthcare Internet of Things (IoT) settings. The high accuracy and low FAR achieved by the CNN-FL model indicate that it can be effectively integrated into existing healthcare systems to enhance their security posture. By leveraging federated learning, “healthcare organizations can improve their intrusion detection capabilities without compromising patient data privacy” (Neyigapula, 2023). This is particularly important given the stringent data protection regulations in the healthcare sector, “such as

Health Insurance Portability and Accountability Act (HIPAA) in the United States and General Data Protection Regulation (GDPR) in the European Union" (Obaid & Salman, 2022).

Additionally, the success of the CNN-FL model in binary and multi-classification tasks not only demonstrates its potential in expanding its applicability to more countries but also its flexibility to be used widely across different subject fields. For example, the models are developed and evaluated using cybersecurity related data, but the model is flexible to evaluate independently across different fields since there is no intrusion detection procedure being coded inside the models.

Chapter 5—Discussion and Conclusions

5.1 Discussion

This praxis aims to enhance cyber threat detection and classification on the Internet of Healthcare Things (IoHT) devices by developing a machine-learning-based intrusion detection system that leverages the combined power of Convolutional Neural Network (CNN) and Federated Learning (FL) machine learning techniques. To this end, questions (RQ) and hypotheses (H) were used to evaluate the effectiveness of the proposed model, as discussed in Chapter 1.

5.1.1 RQ1 and H1: Discussion

The first question posed in this praxis is to determine which federal learning aggregation method can be used as part of the hybrid CNN-FL proposed model developed in this praxis that will yield higher performance. The RQ1 and H1 are as follows:

RQ1: Which federated learning aggregation method, out of Weighted Federated Average (Weighted FedAvg), FedSGD, and FedProx, will achieve the highest accuracy in detecting and classifying cyber threats while preserving data privacy in IoHT devices?

H1: The Weighted FedAvg will achieve a higher accuracy than the FedSGD and FedProx in detecting and classifying cyber threats while preserving data privacy in IoHT devices.

The analysis shows that the weighted FedAvg aggregation method used in the praxis yielded better performance results than the FedSGD and FedProx. Mainly, a

simulated model using the weighted FedAvg aggregation method has an accuracy rate of 97.43%, whereas the FedSGD and FedProx have achieved an accuracy rate of 92.62% and 95.24%, respectively (see Table 4-5). Additionally, the proposed model developed in this praxis using the weighted FedAvg aggregation method has produced a very low false alarm rate (FAR) of 0.5% compared to the other FedSGD and FedProx.

5.1.2 RQ2 and H2: Discussion

The second research question and hypothesis addressed by this praxis are the following:

RQ2: Can a hybrid CNN-federated learning-based model be built to detect and classify cyber threats while preserving patients' privacy in IoHT devices?

H2: A hybrid CNN-federated learning-based model can be built to detect and classify cyber threats while preserving patients' privacy in IoHT devices.

The analysis of the results captured in Table 5-1 shows that the hybrid CNN-FL model for binary classification performed exceptionally well, with higher accuracy, precision, recall, and F1-score above 99 % and a lower FAR rate of 1.42% for 15 clients. The model also achieves similar rates for accuracy with 10 and 5 clients.

For multi-class classification, Table 5-2 shows that the proposed model achieves relatively lower accuracy rates than those obtained in binary classification. The accuracy rate is above 97.00% for the 15, 10, and 5 clients. The precision and recall rates are in the 96.00% range. However, the CNN-FL model shows a significantly lower FAR when classifying potential cyber threats than those in binary classification.

Table 5-1. CNN-FL Binary and Multi-Class Classification Result Summary for 15, 10, and 5 Clients

	Evaluation Metrics	Numbers of Clients		
		15	**10**	**5**
CNN-FL (Binary)	**Accuracy**	0.9920	0.9904	0.9899
	Precision	0.9845	0.9825	0.9824
	Recall	0.9988	0.9995	0.9983
	F1-score	0.9916	0.9910	0.9903
	FAR	0.0142	0.0198	0.0188
CNN-FL (Multiclass)	**Accuracy**	0.9743	0.9760	0.9741
	Precision	0.9636	0.9663	0.9637
	Recall	0.9630	0.9652	0.9628
	F1-score	0.9629	0.9653	0.9625
	FAR	0.0059	0.0055	0.0059

Overall, the analysis of the results confirms the claim made in H2 that a hybrid CNN-federated learning-based model can be built to detect and classify cyber threats while preserving patients' privacy in healthcare IoT networks. Moreover, the analysis shows that the proposed model in this praxis outperforms other FL-based models that used the same or similar datasets, as discussed in the literature review in Chapter 2.

5.1.3 RQ3 and H3: Discussion

The third question posed in the praxis is to determine whether the federated learning model could achieve a higher performance in detecting and classifying multiple cyber threats. The RQ3 and H3 are formulated as follows:

RQ3: Will the proposed model perform better in terms of accuracy, precision, recall, F1 score, and FAR compared to other deep learning-based algorithms, such as CNN, RNN, and DNN, to detect and classify cyber threats while preserving privacy in IoHT devices?

H3: CNN-Federated learning will perform at a higher accuracy, precision, recall, F1 score, and lower false acceptance rate (FAR) than the other deep learning-based algorithms (CNN, RNN, DNN) to detect and classify cyber threats while preserving privacy in IoHT devices.

To determine that the proposed CNN-FL model performed effectively in detecting and classifying cyber threats in IoHT devices, this praxis also examined the performance of the following deep learning models (CNN, RNN, DNN). A quick analysis of the results reveals that the CNN-FL binary classification and DL models have performed at the same level, with an accuracy rate around the 99% range.

However, for multi-class classification, the results show that the selected DL models perform slightly better, with an accuracy rate between 97% and 99%, compared to the CNN-FL model, which achieves an accuracy rate of 97%. This difference in the accuracy rate may be considered insignificant when one considers the privacy-preserving characteristics of the federated learning model, which protects the privacy of patients' data readily available in the healthcare environment.

In summary, it can be concluded that the main goal of this praxis, which is to enhance cyber threat detection and classification in IoHT devices by developing a novel hybrid approach that combines CNN with FL, has been satisfied. The analysis of this study's results has yielded the following key findings.

- The proposed hybrid CNN-Federated Learning model developed in this praxis exhibited a high level of accuracy in detecting cyber threats, with notable precision and recall rates compared to other centralized DL models.
- The model's ability to effectively provide near real-time threat alerts with its potential for proactive threat mitigation in healthcare settings was highlighted in this study through very low FAR rates.
- Federated Learning's privacy-preserving capabilities ensured that sensitive patient data remained protected, which aligned with regulatory requirements.

In addition to these key findings, it is also critical to note that Federated Learning's collaborative nature could contribute to the model's adaptability and scalability, making it a promising solution that healthcare institutions can implement to mitigate cyber threats while preserving privacy in the evolving IoHT environments.

5.2 Conclusion

This praxis successfully developed and evaluated a machine learning-based model utilizing a convolutional neural network and federated learning (CNN-FL) algorithms for the purpose of detecting and classifying cyber threats on the Internet of Healthcare Things (IoHT) devices. The innovative approach of the CNN-FL model using the ECU-IoHT dataset showcased remarkable performance, achieving high levels of accuracy, precision, and recall in various client scenarios. This effectiveness was particularly

evident in its ability to discern between normal and anomalous instances within the ECU-IoHT dataset.

A significant advantage of the federated learning framework was its capability to process data decentralized, which is instrumental in preserving user privacy without compromising the model's predictive efficiency. This aspect is especially crucial in the context of IoHT, where sensitive healthcare data is involved. Regarding computational efficiency, the models demonstrated exceptional speed in both the training and testing phases. This attribute underscores the suitability of our approach for real-time anomaly detection, a critical requirement in IoHT environments where timely response is paramount.

In summary, the results of this research firmly establish the efficacy of using federated learning models to enhance the security of IoHT devices. By effectively guarding against various cyber threats, these models contribute significantly to ensuring the safe and reliable transmission of healthcare data. The study not only underscores the potential of federated learning in IoHT security but also opens avenues for future research in this rapidly evolving field.

5.3 Contributions to Body of Knowledge

As stated in Chapter 1, the main goal of this praxis is to enhance cyber threat detection and classification in IoHT devices by developing a novel hybrid approach that combines CNN with FL. The results of this study have yielded the following findings, which are key contributions to the body of knowledge.

- Innovative model - the proposed hybrid CNN-Federated Learning model developed in this praxis exhibited a high level of accuracy in detecting cyber

threats, with notable precision and recall rates compared to other centralized DL models.

- Effective threat detection and classification - the model's ability to effectively provide near real-time threat alerts with its potential for proactive threat mitigation in healthcare settings was highlighted in this study through very low FAR rates, which previous studies have not reasonably considered. Additionally, this praxis explored multi-class classification, and the results showed that the proposed model can detect and classify multiple cyber threats observed in IoHT environments.
- Privacy-preservation - Federated Learning's privacy-preserving capabilities ensured that sensitive patient data remained protected without negatively impacting the model’s performance, offering a powerful solution that balances security and cyber threat detection.

In addition to these key findings, it is also critical to note that Federated Learning's collaborative nature could contribute to the model's adaptability and scalability, making it a promising solution that healthcare institutions can adopt to mitigate the ever-evolving cyber threats that are noticeable in IoHT devices while preserving privacy.

5.4 Recommendations for Future Research

Despite its potential, the CNN-FL model still has room for improvement for future research. One possible direction is the exploration of more sophisticated federated learning aggregation techniques that handle highly imbalanced and heterogeneous data distributions.

Another future research direction would be to evaluate the CNN-FL model on larger and more diversified datasets. In this study, the CNN-FL model was evaluated based on the ECU-IoHT dataset, which is a very comprehensive dataset. However, it might not cover many different types of cyber threats and data distribution in real-world healthcare IoT environments. Hence, extending the dataset, which includes more types of attacks and data from different healthcare places, is a more thorough evaluation of the effectiveness of this model.

References

Abouzakhar, N. S., Jones, A., & Angelopoulou, O. (2017, June). Internet of things security: A review of risks and threats to healthcare sector. In 2017 IEEE international conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData) (pp. 373-378). IEEE.

Adams, K., (2023). Average Healthcare Data Breach Cost Reaches Nearly $11 Million: https://medcitynews.com/2023/07/healthcare-data-breach-cybersecurity-ransomware/

Ahmad, M. O., & Siddiqui, S. T. (2022). The Internet of Things for healthcare: benefits, applications, challenges, use cases and future directions. In Advances in Data and Information Sciences: Proceedings of ICDIS 2021 (pp. 527-537). Singapore: Springer Singapore.

Ahmad, Z., Shahid Khan, A., Nisar, K., Haider, I., Hassan, R., Haque, M. R., ... & Rodrigues, J. J. (2021). Anomaly detection using deep neural network for IoT architecture. Applied Sciences, 11(15), 7050.

Ahmed, M., Byreddy, S., Nutakki, A., Sikos, L. F., & Haskell-Dowland, P. (2021). ECU-IoHT: A dataset for analyzing cyberattacks in Internet of Health Things. Ad Hoc Networks, 122, 102621.

Akshay Kumaar, M., Samiayya, D., Vincent, P. M., Srinivasan, K., Chang, C. Y., & Ganesh, H. (2022). A Hybrid Framework for Intrusion Detection in Healthcare Systems Using Deep Learning. Frontiers in Public Health, 9, 824898.

Alalhareth, M., & Hong, S. C. (2024). Enhancing the Internet of Medical Things (IoMT) Security with Meta-Learning: A Performance-Driven Approach for Ensemble Intrusion Detection Systems. Sensors, 24(11), 3519.

Alazab, A., Khraisat, A., Singh, S., & Jan, T. (2023). Enhancing Privacy-Preserving Intrusion Detection through Federated Learning. Electronics, 12(16), 3382.

Aledhari, M., Razzak, R., Parizi, R. M., & Saeed, F. (2020). Federated learning: A survey on enabling technologies, protocols, and applications. IEEE Access, 8, 140699-140725.

Al-Hadhrami, S., Vinko, T., Al-Hadhrami, T., Saeed, F., & Qasem, S. N. (2024). Deep learning-based method for sentiment analysis for patients' drug reviews. PeerJ Computer Science, 10, e1976.

Al-Haija, Q. A., McCurry, C. D., & Zein-Sabatto, S. (2021). Intelligent self-reliant cyber-attacks detection and classification system for IoT communication using deep convolutional neural network. In Selected Papers from the 12th International Networking Conference: INC 2020 12 (pp. 100-116). Springer International Publishing.

Alghanmi, A. (2024). An Accurate Disease Classification of COVID-19 and Pneumonia from Chest X-Ray Images Utilizing Mathematical Algorithm-Based Deep Learning Model. Mathematical Modelling of Engineering Problems, 11(4).

Algethami, S. A., & Alshamrani, S. S. (2024). A Deep Learning-Based Framework for Strengthening Cybersecurity in Internet of Health Things (IoHT) Environments. Applied Sciences, 14(11), 4729.

Aljameel, S. S. (2022). A Proactive Explainable Artificial Neural Network Model for the

Early Diagnosis of Thyroid Cancer. Computation, 10(10), 183.

Al-Turaiki, I., & Altwaijry, N. (2021). A Convolutional neural network for improved anomaly-based network intrusion detection. Big Data, 9(3), 233–252. https://doi.org/10.1089/big.2020.0263

Anuar, N. B., Sallehudin, H., Gani, A., & Zakaria, O. (2008). Identifying false alarm for network intrusion detection system using hybrid data mining and decision tree. Malaysian journal of computer science, 21(2), 101-115.

Babbar, H., Rani, S., Singh, A., & Gianini, G. (2023, May). Detecting Cyberattacks to Federated Learning on Software-Defined Networks. In International Conference on Management of Digital (pp. 120-132). Cham: Springer Nature Switzerland.

Balasubramaniam, S., Velmurugan, Y., Jaganathan, D., & Dhanasekaran, S. (2023). A modified LeNet CNN for breast cancer diagnosis in ultrasound images. Diagnostics, 13(17), 2746.

Banerjee, R. (2023). Hands-on TinyML: Harness the Power of Machine Learning on the Edge Devices (English Edition). BPB Publications.

Basharat, A., Mohamad, M. M. B., & Khan, A. (2022, July). Machine learning techniques for intrusion detection in Smart Healthcare Systems: A comparative analysis. In 2022 4th International Conference on Smart Sensors and Application (ICSSA) (pp. 29-33). IEEE.

Bhavsar, M., Roy, K., Kelly, J., & Olusola, O. (2023). Anomaly-based intrusion detection system for IoT application. Discover Internet of Things, 3(1), 5.

Behrooz, S., & Marsh, S. (2016). A trust-based framework for information sharing between mobile health care applications. In Trust Management X: 10th IFIP WG

11.11 International Conference, IFIPTM 2016, Darmstadt, Germany, July 18-22, 2016, Proceedings 10 (pp. 79-95). Springer International Publishing.

Bensaid, R., Labraoui, N., Abba Ari, A. A., Maglaras, L., Saidi, H., Abdu Lwahhab, A. M., & Benfriha, S. (2024). Toward a Real-Time TCP SYN Flood DDoS Mitigation Using Adaptive Neuro-Fuzzy Classifier and SDN Assistance in Fog Computing. Security and Communication Networks, 2024(1), 6651584.

Bera, S., Misra, S., & Vasilakos, A. V. (2017). Software-defined networking for internet of things: A survey. IEEE Internet of Things Journal, 4(6), 1994-2008.

Binbusayyis, A., Alaskar, H., Vaiyapuri, T., & Dinesh, M. (2022). An investigation and comparison of machine learning approaches for intrusion detection in IoMT network. The Journal of Supercomputing, 78(15), 17403-17422.

Birchha, V., & Nigam, B. (2022). Data Splitting Techniques to Reduce False-Positive and False? Negative Cases in Breast Cancer Prediction. NeuroQuantology, 20(8), 9410.

Bonawitz, K., Eichner, H., Grieskamp, W., Huba, D., Ingerman, A., Ivanov, V., ... & Roselander, J. (2019). Towards federated learning at scale: System design. Proceedings of machine learning and systems, 1, 374-388.

Boriah, S., Chandola, V., & Kumar, V. (2008, April). Similarity measures for categorical data: A comparative evaluation. In Proceedings of the 2008 SIAM international conference on data mining (pp. 243-254). Society for Industrial and Applied Mathematics.

Butt, S. A., Diaz-Martinez, J. L., Jamal, T., Ali, A., De-La-Hoz-Franco, E., & Shoaib, M. (2019, July). IoT smart health security threats. In 2019 19th International

conference on computational science and its applications (ICCSA) (pp. 26-31). IEEE.

Chaganti, R., Mourade, A., Ravi, V., Vemprala, N., Dua, A., & Bhushan, B. (2022). A particle swarm optimization and deep learning approach for intrusion detection system in internet of medical things. Sustainability, 14(19), 12828.

Chakraborty, C., Pani, S., Ahad, M. A., & Xin, Q. (Eds.). (2022). Implementation of Smart Healthcare Systems Using AI, IoT, and Blockchain. Academic Press.

Cheng, Y., Wang, D., Zhou, P., & Zhang, T. (2017). A survey of model compression and acceleration for deep neural networks. arXiv preprint arXiv:1710.09282.

Dang, L. M., Piran, M. J., Han, D., Min, K., & Moon, H. (2019). A survey on internet of things and cloud computing for healthcare. Electronics, 8(7), 768.

Dasu, T., & Johnson, T. (2003). Exploratory data mining and data cleaning. John Wiley & Sons.

Deming, C., Dekkati, S., & Desamsetti, H. (2018). Exploratory Data Analysis and Visualization for Business Analytics. Asian Journal of Applied Science and Engineering, 7(1), 93-100.

Djenna, Amir, Saad Harous, and Djamel Eddine Saidouni. (2021). "Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure" Applied Sciences 11, no. 10: 4580. https://doi.org/10.3390/app11104580

Dixit, P., & Silakari, S. (2021). Deep learning algorithms for cybersecurity applications: A technological and status review. Computer Science Review, 39, 100317. https://doi.org/10.1016/j.cosrev.2020.100317

Duy, P. T., Van Hung, T., Ha, N. H., Do Hoang, H., & Pham, V. H. (2021, December). Federated learning-based intrusion detection in SDN-enabled IIoT networks. In 2021 8th NAFOSTED Conference on Information and Computer Science (NICS) (pp. 424-429). IEEE.

Elgayar, S. M., Hamad, S., & El-Horbaty, E. S. M. (2023). Revolutionizing Medical Imaging through Deep Learning Techniques: An Overview. International Journal of Intelligent Computing and Information Sciences, 23(3), 59-72.

Eshan, M., Nafi, M. N. H., Sakib, N., Maruf, M. A. M., & Emon, M. H. (2023). A secured federated learning system leveraging confidence score to identify retinal disease (Doctoral dissertation, Brac University).

Ferrag, M. A., Friha, O., Maglaras, L., Janicke, H., & Shu, L. (2021). Federated deep learning for cyber security in the internet of things: Concepts, applications, and experimental analysis. IEEE Access, 9, 138509-138542.

Gafni, T., Shlezinger, N., Cohen, K., Eldar, Y. C., & Poor, H. V. (2022). Federated learning: A signal processing perspective. IEEE Signal Processing Magazine, 39(3), 14-41.

Ghadi, Y. Y., Mazhar, T., Shah, S. F. A., Haq, I., Ahmad, W., Ouahada, K., & Hamam, H. (2023). Integration of federated learning with IoT for smart cities applications, challenges, and solutions. PeerJ Computer Science, 9, e1657.

Ghimire, B., & Rawat, D. B. (2022). Recent advances in federated learning for cybersecurity and cybersecurity for federated learning for the Internet of Things. IEEE Internet of Things Journal, 9(11), 8229-8249. https://doi.org/10.1109/jiot.2022.3150363

Ghourabi, M., Mourad-Chehade, F., & Chkeir, A. (2024). Advancing Cough Classification: Swin Transformer vs. 2D CNN with STFT and Augmentation Techniques. Electronics, 13(7), 1177.

Goud, N (2019, April 17). *Malware and ransomware attack on medical devices – Cybersecurity Insiders*. Cybersecurity Insiders. https://www.cybersecurity-insiders.com/malware-and-ransomware-attack-on-medical-devices/

Hagras, E. A., Aldosary, S., Khaled, H., & Hassan, T. M. (2023). Authenticated Public Key Elliptic Curve Based on Deep Convolutional Neural Network for Cybersecurity Image Encryption Application. Sensors, 23(14), 6589.

Hu, Y., Liu, R., & Ma, Z. (2021). Identification of cybersecurity elements based on convolutional attention LSTM networks. In Journal of Physics: Conference Series (Vol. 1757, No. 1, p. 012146). IOP Publishing.

Hussain, F., Abbas, S. G., Shah, G. A., Pires, I. M., Fayyaz, U. U., Shahzad, F., ... & Zdravevski, E. (2021). A framework for malicious traffic detection in IoT healthcare environment. Sensors, 21(9), 3025.

Judith, A., Kathrine, G. J. W., & Silas, S. (2023). Efficient Deep Learning-Based Cyber-Attack Detection for Internet of Medical Things Devices. Engineering Proceedings, 59(1), 139.

Kaur, K., Kaur, A., Gulzar, Y., & Gandhi, V. (2024). Unveiling the core of IoT: comprehensive review on data security challenges and mitigation strategies. Frontiers in Computer Science, 6, 1420680.

Kim, J., Kim, J., Thu, H. L. T., & Kim, H. (2016, February). Long short-term memory recurrent neural network classifier for intrusion detection. In 2016 international

conference on platform technology and service (PlatCon) (pp. 1-5). IEEE.

Kim, J., Kim, J., Kim, H., Shim, M., & Choi, E. (2020). CNN-based network intrusion detection against denial-of-service attacks. Electronics, 9(6), 916.

Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2017). ImageNet classification with deep convolutional neural networks. Communications of the ACM, 60(6), 84-90.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1), 1-10.

Lakshmanamoorthy, R. (2021, October 13). Getting started with deep learning using TensorFlow Keras. Analytics India Magazine. https://analyticsindiamag.com/deep-learning-using-tensorflow-keras/

Le, A. T., Shakiba, M., & Ardekani, I. (2024). Tomato disease detection with lightweight recurrent and convolutional deep learning models for sustainable and smart agriculture. Frontiers in Sustainability, 5, 1383182.

Lee, J. D., Cha, H. S., Rathore, S., & Park, J. H. (2021). M-IDM: A Multi-Classification Based Intrusion Detection Model in Healthcare IoT. Computers, Materials & Continua, 67(2).

Lee, B. S., Kim, J. W., & Choi, M. J. (2023, September). Federated Learning Based Network Intrusion Detection Model. In 2023 24st Asia-Pacific Network Operations and Management Symposium (APNOMS) (pp. 330-333). IEEE

Li, H. B. (2014). Knowledge discovering in corporate securities fraud by using grammar based genetic programming. Journal of Computer and Communications, 2(04), 148.

Lyell, D., Coiera, E., Chen, J., Shah, P., & Magrabi, F. (2021). How machine learning is embedded to support clinician decision making: an analysis of FDA-approved medical devices. BMJ health & care informatics, 28(1).

Malik, F., Waqas Khan, Q., Rizwan, A., Alnashwan, R., & Atteia, G. (2024). A Machine Learning-Based Framework with Enhanced Feature Selection and Resampling for Improved Intrusion Detection. Mathematics, 12(12), 1799.

Maurício, J., Domingues, I., & Bernardino, J. (2023). Comparing vision transformers and convolutional neural networks for image classification: A literature review. Applied Sciences, 13(9), 5521.

McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017, April). Communication-efficient learning of deep networks from decentralized data. In Artificial intelligence and statistics (pp. 1273-1282). PMLR.

Mehdary, A., Chehri, A., Chehri, A., Jakimi, A., & Saadane, R. (2024). Hyperparameter Optimization with Genetic Algorithms and XGBoost: A Step Forward in Smart Grid Fraud Detection. Sensors, 24(4), 1230.

Montero, C. D. L., Gundul, B. J. A., Frayco, J. G., & Candia Jr, J. Q. (2023). Convolutional Neural Network-based Image Classification for Improved Coconut Disease Identification. SDSSU Multidisciplinary Research Journal, 11(1), 17-21.

Mosaiyebzadeh, F., Pouriyeh, S., Parizi, R. M., Han, M., & Batista, D. M. (2023, May). Intrusion Detection System for IoHT Devices using Federated Learning. In IEEE INFOCOM 2023-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 1-6). IEEE.

Musleh, D., Alotaibi, M., Alhaidari, F., Rahman, A., & Mohammad, R. M. (2023).

Intrusion detection system using feature extraction with machine learning algorithms in IoT. Journal of Sensor and Actuator Networks, 12(2), 29.

Nedeljkovic, D., & Jakovljevic, Z. (2022). CNN-based method for the development of cyber-attack detection algorithms in industrial control systems. Computers & Security, 114, 102585. https://doi.org/10.1016/j.cose.2021.102585

Neyigapula, B. S. (2023). Federated Learning for Collaborative Network Security in Decentralized Environments. J Sen Net Data Comm, 3(1), 81-92.

Ntizikira, E., Lei, W., Alblehai, F., Saleem, K., & Lodhi, M. A. (2023). Secure and privacy-preserving intrusion detection and prevention in the internet of unmanned aerial vehicles. Sensors, 23(19), 8077.

Obaid, H. S., Dheyab, S. A., & Sabry, S. S. (2019, March). The impact of data pre-processing techniques and dimensionality reduction on the accuracy of machine learning. In 2019 9th annual information technology, electromechanical engineering and microelectronics conference (iemecon) (pp. 279-283). IEEE.

Obaid, O. I., & Salman, S. A. B. (2022). Security and privacy in IoT-based healthcare systems: a review. Mesopotamian Journal of Computer Science, 2022, 29-39.

Odeyemi, O., Mhlongo, N. Z., Nwankwo, E. E., & Soyombo, O. T. (2024). Reviewing the role of AI in fraud detection and prevention in financial services. International Journal of Science and Research Archive, 11(1), 2101-2110.

Okey, O. D., Maidin, S. S., Adasme, P., Lopes Rosa, R., Saadi, M., Carrillo Melgarejo, D., & Zegarra Rodríguez, D. (2022). BoostedEnML: Efficient technique for detecting cyberattacks in IoT systems using boosted ensemble machine learning. Sensors, 22(19), 7409.

Otoum, Y., Wan, Y., & Nayak, A. (2021, December). Federated transfer learning-based ids for the internet of medical things (iomt). In 2021 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE

Patil, P. (2022, May 30). What is Exploratory Data Analysis? - Towards Data Science. Medium. https://towardsdatascience.com/exploratory-data-analysis-8fc1cb20fd15

Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2013). Context aware computing for the internet of things: A survey. IEEE communications surveys & tutorials, 16(1), 414-454.

Poenicke, O., Groneberg, M., & Richter, K. (2019). Method for the planning of IoT use cases in Smart Logistics Zones. IFAC-PapersOnLine, 52(13), 2449-2454.

Prusty, S., Patnaik, S., & Dash, S. K. (2022). SKCV: Stratified K-fold cross-validation on ML classifiers for predicting cervical cancer. Frontiers in Nanotechnology, 4, 972421.

Qiang, G. (2022). Research on software vulnerability detection method based on improved CNN model. Scientific Programming, 2022.

Radford, A., Metz, L., & Chintala, S. (2015). Unsupervised representation learning with deep convolutional generative adversarial networks. arXiv preprint arXiv:1511.06434.

Rahman, A., Hossain, M. S., Muhammad, G., Kundu, D., Debnath, T., Rahman, M., ... & Band, S. S. (2023). Federated learning-based AI approaches in smart healthcare: concepts, taxonomies, challenges and open issues. Cluster computing, 26(4), 2271-2311.

Rashid, M.M., Khan, S.U., Eusufzai, F., Redwan, M.A., Sabuj, S.R., & Elsharief, M.

(2023). A Federated Learning-Based Approach for Improving Intrusion Detection in Industrial Internet of Things Networks. Network, 3, 158-179.

Saheed, Y. K., & Arowolo, M. O. (2021). Efficient cyber-attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms. IEEE Access, 9, 161546-161554.

Saleh, H. M., Marouane, H., & Fakhfakh, A. (2024). A Comprehensive Analysis of Security Challenges and Countermeasures in Wireless Sensor Networks Enhanced by Machine Learning and Deep Learning Technologies. International Journal of Safety & Security Engineering, 14(2).

Sarker, I. H., Khan, A. I., Abushark, Y. B., & Alsolami, F. (2023). Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. Mobile Networks and Applications, 28(1), 296-312.

Seung-Jun, L. (2020). A Preprocessing Strategy for Denoising of Speech Data Based on Speech Segment Detection. Applied Sciences, 10(20), 7385.

Sharma, G. (2017). Pros and cons of different sampling techniques. International journal of applied research, 3(7), 749-752.

Sharma, N., Jain, V., & Mishra, A. (2018). An analysis of convolutional neural networks for image classification. Procedia computer science, 132, 377-384.

Si-Ahmed, A., Al-Garadi, M. A., & Boustia, N. (2024). Explainable Machine Learning-Based Security and Privacy Protection Framework for Internet of Medical Things Systems. arXiv preprint arXiv:2403.09752.

Sittig, D. F., & Singh, H. (2016). A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. Applied clinical informatics, 7(02),

624-632.

Sommer, R., & Paxson, V. (2010, May). Outside the closed world: On using machine learning for network intrusion detection. In 2010 IEEE symposium on security and privacy (pp. 305-316). IEEE.

Sue, P., (2023). Cost of Data Breach 2023: Pharmaceutical Industry Impacts, https://securityintelligence.com/articles/cost-of-a-data-breach-2023-pharmaceutical-industry/

Tang, Y., Zhang, Y., Niu, T., Li, Z., Zhang, Z., Chen, H., & Zhang, L. (2024). A Survey on Blockchain-Based Federated Learning: Categorization, Application and Analysis. CMES-Computer Modeling in Engineering & Sciences, 139(3).

Tauqeer, H., Iqbal, M. M., Ali, A., Zaman, S., & Chaudhry, M. U. (2022). Cyberattacks Detection in IoMT using Machine Learning Techniques. Journal of Computing & Biomedical Informatics, 4(01), 13-20.

Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102.

Thamer, N., & Alubady, R. (2021, April). A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research. In 2021 1st Babylon International Conference on Information Technology and Science (BICITS) (pp. 210-216). IEEE.

Thamilarasu, G., Odesile, A., & Hoang, A. (2020). An intrusion detection system for internet of medical things. IEEE Access, 8, 181560-181576.

UrRehman, Z., Qiang, Y., Wang, L., Shi, Y., Yang, Q., Khattak, S. U., ... & Zhao, J. (2024). Effective lung nodule detection using deep CNN with dual attention

mechanisms. Scientific Reports, 14(1), 3934.

Verma, H., Kumar, A., Mishra, G. S., Mishra, P. K., & Nand, P. (2022). DRIVER DROWSINESS DETECTION. NeuroQuantology, 20(22), 3179.

Vijayakumar, K. P., Pradeep, K., Balasundaram, A., & Prusty, M. R. (2023). Enhanced Cyber Attack Detection Process for Internet of Health Things (IoHT) Devices Using Deep Neural Network. Processes, 11(4), 1072. https://doi.org/10.3390/pr11041072

Wang, Y. (2017). Feature extraction and feature evaluation framework for document representation. https://core.ac.uk/download/577479555.pdf

Wu, Y., Kang, Y., Luo, J., He, Y., & Yang, Q. (2021). Fedcg: Leverage conditional gan for protecting privacy and maintaining competitive performance in federated learning. arXiv preprint arXiv:2111.08211.

Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. International Journal of Information Security, 21(1), 115-158.

Yadav, M. K., & Sharma, K. P. (2021, May). Intrusion detection system using machine learning algorithms: a comparative study. In 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC) (pp. 415-420). IEEE.

Yuan, N., Yang, W., Kang, B., Xu, S., & Wang, X. (2018). Laplacian Eigenmaps Feature Conversion and Particle Swarm Optimization-Based Deep Neural Network for Machine Condition Monitoring. Applied Sciences, 8(12), n/a.

Zahra, S., Ghazanfar, M. A., Khalid, A., Azam, M. A., Naeem, U., & Prugel-Bennett, A.

(2015). Novel centroid selection approaches for KMeans-clustering based recommender systems. Information sciences, 320, 156-189.

Zhang, W., Zhao, Y., Li, F., & Zhu, H. (2023). A Hierarchical Federated Learning Algorithm Based on Time Aggregation in Edge Computing Environment. Applied Sciences, 13(9), 5821.