Shailender Kumar

Ashish_thesis_report

paper

Document Details

Submission ID

trn:oid:::27535:143873563

Submission Date

Jun 22, 2026, 2:29 PM GMT+5:30

Download Date

Jun 22, 2026, 2:33 PM GMT+5:30

File Name

Ashish_thesis_report.pdf

File Size

12.5 MB

62 Pages

13,810 Words

82,151 Characters

4% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text
- Small Matches (less than 14 words)

Match Groups

16 Not Cited or Quoted 4%
Matches with neither in-text citation nor quotation marks

0 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

3% Internet sources
0% Publications
3% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- **16** Not Cited or Quoted 4%
  Matches with neither in-text citation nor quotation marks
- **0** Missing Quotations 0%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

3% Internet sources
0% Publications
3% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	www.dspace.dtu.ac.in:8080	1%
2	Student papers	Delhi Technological University on 2026-06-09	<1%
3	Student papers	Delhi Technological University on 2026-06-01	<1%
4	Student papers	University of Wollongong on 2023-12-07	<1%
5	Internet	vdocuments.mx	<1%
6	Student papers	Alliance College of Engineering and Design on 2025-11-03	<1%
7	Internet	pmc.ncbi.nlm.nih.gov	<1%
8	Internet	www.mdpi.com	<1%
9	Student papers	University of Hertfordshire on 2023-03-09	<1%
10	Internet	infinitylearn.com	<1%

11 Student papers

Delhi Technological University on 2026-05-28 <1%

12 Internet

mscest.cut.ac.cy <1%

13 Student papers

Asia Pacific University College of Technology and Innovation (UCTI) on 2025-09-19 <1%

14 Student papers

Glasgow Caledonian University on 2026-04-16 <1%

15 Internet

baadalsg.inflibnet.ac.in <1%

DL-BASED INTRUSION DETECTION FOR IOMT: A COMPARATIVE ANALYSIS OF EMBED-NET, CONV-NET-SVM, AND DEEP-SVM-NET

A PROJECT REPORT

1

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE
OF

MASTER OF TECHNOLOGY
IN
COMPUTER SCIENCE AND ENGINEERING

Submitted by

ASHISH KUMAR

2K24/CSE/12

Under the supervision of

Prof. Shailender Kumar

THE DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi 110042

MAY, 2026

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CANDIDATE'S DECLARATION

I, Ashish Kumar, Roll No. 2K24/CSE/12 student of M.Tech (Computer Science and Engineering),hereby declare that the project Dissertation titled "**DL-BASED INTRUSION DETECTION FOR IOMT: A COMPARATIVE ANALYSIS OF EMBED-NET, CONV-NET-SVM, AND DEEP-SVM-NET**" which is submitted by me to the Department of Computer Science and Engineering, Delhi Technological University, Delhi in partial fulfilment of the requirement for the award of degree of Master of Technology, is original and not copied from any source without proper citation. This work has not previously formed the basis for the award of any Degree, Diploma Associateship, Fellowship or other similar title or recognition.

Place: Delhi **Ashish Kumar**

Date: **2k24/CSE/12**

This is to certify that the student has incorporated all the corrections suggested by the examiners in the thesis and the statement made by the candidate is correct to the best of our knowledge.

Signature of Supervisor **Signature of External Examiner**

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CERTIFICATE BY SUPERVISOR

Certified that **Ashish Kumar**(2K24/CSE/12) has carried out their research work presented in this thesis entitled **"DL-BASED INTRUSION DETECTION FOR IOMT: A COMPARATIVE ANALYSIS OF EMBED-NET, CONV-NET-SVM, AND DEEP-SVM-NET"** for the award of **Master of Technology** from Department of Computer Science and Engineering, Delhi Technological University, Delhi, under my supervision. The thesis embodies results of original work, and studies are carried out by the student himself and the contents of the thesis do not form the basis for the award of any other degree to the candidate or to anybody else from this or any other University/Institution.

Place: Delhi

Date:

Prof. Shailender Kumar
SUPERVISOR
(Professor, CSE, DTU)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

ACKNOWLEDGEMENT

I am grateful to Prof. SHAILENDER KUMAR, Professor, Department of Computer Science and Engineering, and all the faculty members at Delhi Technological University for their guidance and support throughout the seminar. I would like to extend my heart-felt gratitude to Prof. Anil Singh Parihar, Head of the Department, Computer Science and Engineering, Delhi Technological University, for his continuous guidance, motivation, unwavering encouragement and invaluable insights. I appreciate the support provided by the University, including the laboratories, infrastructure, testing facilities, and environment that enabled me to work without interruption. I thank my lab assistants, seniors, and peer group for their aid and knowledge on various subjects. I am also grateful to everyone who directly or indirectly contributed to the completion of this project, and my parents and well-wishers for their constant support, belief in me, and encouragement.

Ashish Kumar

2k24/CSE/12

ABSTRACT

The swift development of IoMT technology has led to the ability of continuously tracking patients, automating clinical operations, and facilitating interaction between connected devices in contemporary healthcare settings. While these interrelated processes greatly improve medical efficiency and accessibility, there are major cybersecurity risks present as well. Typically, medical devices have low computing power, run outdated firmware, and lack sophisticated protection systems; therefore, they become easy targets for diverse cyber attacks such as DoS [7], reconnaissance, spoofing, and data manipulation attacks. It turns out to be hard to cope with dynamic and sophisticated IoMT traffic using common IDS technologies [8], like signature-based IDS and traditional machine learning techniques. The limitations of the existing systems in terms of poor adaptiveness, simplified feature representation, and high levels of false negatives prove the necessity of further research in creating smart IDS techniques.

This study introduces a 3-part deep learning solution specifically for an IoMT IDS – Embed-Net, Conv-Net-SVM, and Deep-SVM-Net. Each model is a solution to specific security problems with IoMT environment. Embed-Net is an approach that embeds device identifiers, flags, and protocol attributes into dense models that are learned from the data and enables these models to represent subtle interactions between heterogeneous network traffic. The Conv-Net-SVM performed convolutional feature extraction followed by a Support Vector Machine (SVM) classifier, fusing the advantages of CNN, which is capable of learning the structs in the flow with good margin-based decision boundaries of SVM. Deep-SVM-Net is an output layer based on SVM that exploits a novel approach to deep neural net that functions well in separating benign and malicious traffic and simultaneously has a low computational load for resource constrained medical devices.

Several IoT-related datasets that included the various cyber-attack patterns were first preprocessed for standardization of scaling, transformations to ordinal encoding, feature selection based on covariance, and SMOTE balancing before training and validation were performed on the datasets, each using a cross validation strategy that ensured stable and generalizable models. All three exhibited excellent intrusion detection results with particularly good overall accuracy and low false-negative rates from Embed-Net, outstanding capability in learning attack signatures with high spatial correlations from ConvNetSVM, and superior intrusion detection real-time efficiency with highly reliable binary separation from Deep-SVM-Net. The results collectively point to the superiority of the deep learn-

ing architecture for improving the security of IoMT, which efficiently adapts to mixed-type features, to an imbalanced dataset, and to medical operational constraints.

5

TABLE OF CONTENTS

Contents

Candidate's Declaration **i**

Certificate **ii**

Acknowledgement **iii**

Abstract **iv**

Table of Contents **viii**

List of Figures **ix**

List of Tables **x**

CHAPTER 1: INTRODUCTION **1**

1.1 Evolution of IoMT in Modern Healthcare 2

1.2 Security Challenges in IoMT Environments 3

CHAPTER 2: RELATED WORK **6**

2.1 Traditional and Machine Learning-based IDS Approaches 6

2.2 Deep Learning Approaches to IoMT Intrusion Detection 7

2.3 Challenges in Developing IDS for IoMT Environments 8

2.4 Importance of Dataset Quality in IoMT Intrusion Detection 10

2.5 Prior Research on IoMT Intrusion Detection 11

CHAPTER 3: METHODOLOGY **16**

3.1 Data Preparation and Preprocessing Pipeline 17

3.1.1 Cleaning the Dataset and Removing Redundancy 18

3.1.2 Missing Value Imputation 19

3.1.3 Encoding of Categorical Features 19

3.1.4 Normalization and Transformation of Numerical Attributes 19
3.1.5 Handling Class Imbalance Using SMOTE 20
3.1.6 Data-set Splitting & Cross-Validation 20
3.2 Architecture of Proposed Models 20
3.2.1 Embed-Net: Embedding-Based Deep Learning Architecture 20
3.2.2 Conv-Net-SVM: Hybrid Convolution + Margin Classifier 22
3.2.3 Deep-SVM-Net: Deep Neural Network with Margin-Based Classification 25
3.2.4 Regularization Techniques 26
3.2.5 Cross-Dataset Generalization 27
3.3 Feature Engineering and Dimensional Optimization 27
3.4 Training Strategy and Model Optimization 28
3.5 Real-Time Deployment Considerations for IoMT IDS 29

CHAPTER 4: RESULTS AND DISCUSSION 31
4.1 Evaluation Metrics and Experimental Setup 31
4.2 Embed-Net: Results and Interpretation 32
4.2.1 Accuracy and Detection Performance 32
4.2.2 Training Behavior and Convergence Trends 32
4.2.3 Computational Considerations 32
4.3 Conv-Net-SVM: Results and Interpretation 33
4.3.1 Accuracy and Structural Pattern Recognition 33
4.3.2 Convergence Stability and Epoch Analysis 33
4.3.3 Effect of Batch Sizes 33
4.3.4 Computational Efficiency 37
4.4 Deep-SVM-Net: Results and Interpretation 38
4.4.1 Accuracy and Margin Optimization 38
4.4.2 Training and Validation Behavior 38
4.4.3 Efficiency and Deployment Readiness 38
4.5 Comparative Discussion of All Three Models 39
4.5.1 Overall Accuracy 39
4.5.2 False-Negative Rates 39
4.5.3 Computational Efficiency 39
4.5.4 Semantic Categorical Feature Understanding 40

6 **CHAPTER 5: CONCLUSION AND FUTURE SCOPE** **41**

5.1 Conclusion 41

5.2 Practical Implications of the Proposed IDS Framework 42

5.3 Limitations of the Present Study 43

5.4 Future Scope 45

LIST OF FIGURES

FIGURE NO.	DESCRIPTION	PAGE NO.
Figure 1.1	IoMT architecture.	2
Figure 3.1	Overall workflow of the proposed IoMT intrusion detection framework integrating preprocessing, deep learning architectures, and evaluation stages.	17
Figure 3.2	Experimental workflow of the proposed framework for attack detection in IoMT environments.	18
Figure 3.3	Architecture of Embed-Net model.	21
Figure 3.4	Architecture of Conv-Net-SVM model.	23
Figure 3.5	Architecture of Deep-SVM-Net model.	25
Figure 4.1	Training curves (Epoch = 100, Batch = 64).	34
Figure 4.2	Training curves (Epoch = 100, Batch = 128).	35
Figure 4.3	Training curves (Epoch = 100, Batch = 256).	36

LIST OF TABLES

TABLE NO.	DESCRIPTION	PAGE NO.
Table 4.1	Cross-dataset performance of the proposed IoMT intrusion detection models.	27

LIST OF ABBREVIATIONS

ABBREVIATION	DEFINITION
IoMT	Internet of Medical Things
IDS	Intrusion Detection System
CNN	Convolutional Neural Network
SVM	Support Vector Machine
DoS	Denial of Service
DDoS	Distributed Denial of Service
AE	Autoencoder
SMOTE	Synthetic Minority Over-sampling Technique
RNN	Recurrent Neural Network
LSTM	Long Short-Term Memory
GRU	Gated Recurrent Unit
DNN	Deep Neural Network
MITM	Man-in-the-Middle
ML	Machine Learning
BN	Batch Normalization
GPU	Graphics Processing Unit
ICU	Intensive Care Unit
ROC	Receiver Operating Characteristic
FNR	False Negative Rate
AI	Artificial Intelligence

Chapter 1

INTRODUCTION

The vast growth of science and technology in the medical field, where devices are increasingly linked to the Internet, is revolutionizing the medical field. Popularly known as the Internet of Medical Things, these connected gadgets allow real-time patient tracking, remote diagnosis, taking care of medications, telemedicine, as well as smooth medical information interaction within medical centers and among medical care suppliers. IoMT is a multi-layered system in which devices connect to gateways, the cloud, and clinical decision support systems. In addition to this growing digital infrastructure being a powerful enabler for the provision of care, it has also raised new and significant cybersecurity risks.

Traditional IDSs[28] have fallen short in protecting IoMT environments. Signature-based IDSs can detect only those attacks whose patterns already exist in their signature databases, failing to identify zero-day exploits or novel attack variants. Anomaly-based IDSs are more flexible but often suffer from high false-positive rates due to the natural variability and non-stationarity of the medical network traffic. While ML provided extra flexibility, many ML-based IDSs rely on a broad manual feature engineering process, often failing when confronting typical IoMT datasets characterized by strong heterogeneity, high dimensionality, and pronounced class imbalance. These challenges point toward the need for intelligent deep learning models that can independently learn complex patterns, adapt to the evolving threats, and be computationally feasible for real-world deployments.

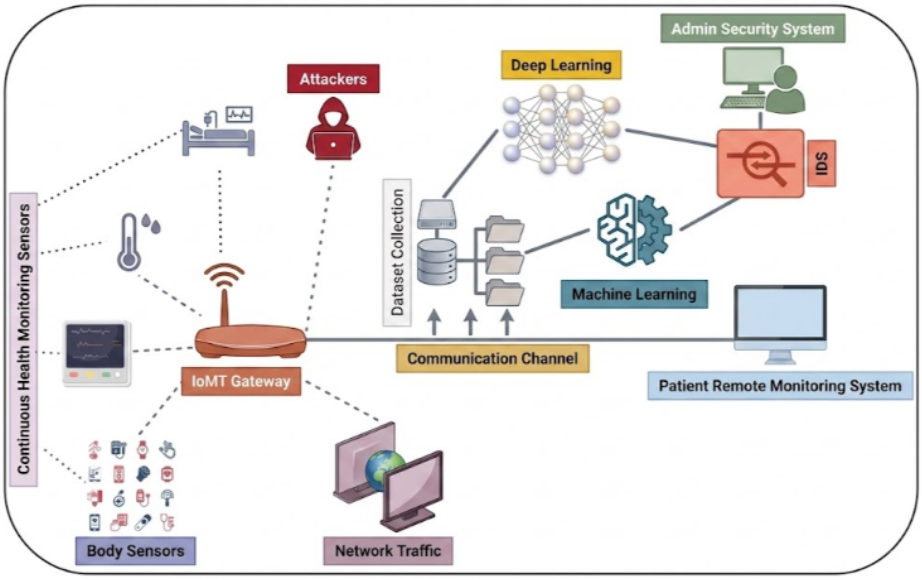


Figure 1.1: IoMT architecture.

1.1 Evolution of IoMT in Modern Healthcare

The healthcare industry has experienced a major transformation with the rapid adoption of interconnected digital technologies. Earlier healthcare systems primarily depended on manual monitoring, isolated medical equipment, and delayed communication between healthcare providers and patients. However, the emergence of the Internet of Medical Things (IoMT) has been significantly changed the process of medical services are delivered, monitored, and also managed.

IoMT is an end-to-end system of medical devices, wearable sensors, health applications, communication gateways and the cloud, which share medical data continuously via the internet. These integrated systems are able to monitor physiological parameters including heart-rate, blood-pressure, glucose, oxygen-saturation, and body-temperature, all in real-time. The gathered data is sent to health care providers enabling prompt diagnosis and medical decisions.

The capacity to remotely transmit patient data and instructions, the development of embedded systems, and the expansion of Cloud Computing and AI have helped make the IoMT infrastructures increasingly widespread within hospitals, clinics, diagnostic centers, and Domotics environments. Smart healthcare devices such as smart wearables, remote patient monitoring systems, robotic surgery systems and smart infusion pumps are becoming common features of the modern health care system.

One of the main advantages of IoMT lies in the ability to provide continuous patient supervision beyond traditional hospital boundaries. Patients suffering from the chronic diseases, cardiovascular diseases, diabetes, and age-related conditions can now receive personalized healthcare services remotely. This has been reduced hospitalizational costs, minimized unnecessary of clinical visits, and improved the healthcare accessibility in the rural as well as remote regions.

The pandemic outbreak of the Covid-19 further highlighted the importances of such technologies in the IoMT. When movement was severely very limited and health care services were almost overstretched, remote monitoring and telehealth enabled health care providers to continue providing care. Consequently, health care institutions around the globe sped up investments in digital health-care infrastructure.

However, with these benefits also with IoMT comes an increase in the size of the attack surface for cyber threats. Many medical devices have insecure systems and outdated security platforms, and can be targeted by malicious attacks, unauthorized access and data manipulation. As such, the need for cybersecurity in IoMT systems is growing rapidly to guarantee reliable healthcare delivery and patient safety.

1.2 Security Challenges in IoMT Environments

While IoMT has brought the healthcare sector greater efficiency and accessibility, it has also brought with it critical cybersecurity issues. Medical devices constantly transmit highly sensitive patient data on a network of interconnected devices, making them easy prey for cybercriminals. The privacy, integrity, and availability of patient medical information could directly impact clinical operations and patient safety.

Low computational power of medical devices is one of the most significant issues of IoMT systems. Many wearable sensors, portable monitoring devices and embedded healthcare systems are engineered to have very little processing power and memory to minimize energy usage and operational costs. This means that these devices are often not equipped with the advanced security features that you would expect.In consequence, these devices are frequently susceptible to cyberattacks.

DDoS attacks are considered to be among the very devastating forms of cyber-attacks on healthcare infra-structure. DDoS involves flooding health-care servers with a significant amount of traffic through compromised devices under the control of hackers. In case

of the MITM attacks, the hackers interrupt the communication flow between two devices or between a single device and also the health-care server, hence compromising sensitive information.

The use of ransomware attacks has become common within the health care industry. Such an attack involves the encryption of important data stored in a hospital database or the interference with the infrastructure of a health-care organization that comes to a stop until the demanded ransom is received.

Another bigger problem is that of hetero-geneity within the IoMT environment. Networks for healthcare contain devices of various makes, which have different the protocols, operating systems, and data formats. It becomes very challenging to ensure uniform security policies and intrusion detection mechanisms when there are hetero-geneous devices in the network.

The traditional security methods are of used to prevent attacks on computer networks can be ineffective because of their reliance on attack signature rules. These approaches struggle to identify zero-day attacks and evolving intrusion patterns commonly observed in modern cyber warfare. Consequently, intelligent intrusion detection systems capable of adaptive learning and real-time threat analysis have become essential for securing IoMT infrastructures.

Embed-Net implements categorical embedding layers to map symbolic IoMT attributes, including device identifiers, port information, connection flags, and protocol types, into a compact dense vector form for better semantic relationships among categorical values and therefore more expressive and compact feature representation of network flow. Figure 2 depicts how the architecture can combine embedding vectors with continuous numerical features in one coherent learning framework.

Conv-Net-SVM brings together the strengths of a ConvNet in feature extraction and the margin-based decision mechanism of an SVM. Spatial and structural patterns in IoMT traffic-which may manifest, for instance, as periodic behaviors in flow-level statistics-are automatically detected by the convolutional layers, while the separation between benign and malicious flows is driven by the SVM layer to guarantee a large-margin separation. As shown in Figure 3, the convolutional feature maps feed into a hybrid SVM decision layer. This hybridization works really well for recognizing patterned attacks, such as DDoS bursts or periodic probing sequences.

Deep-SVM-Net uses deep fully connected neural networks to build a powerful nonlin-

ear feature space and augments it with an SVM-inspired output layer that enforces tighter decision margins, as depicted in Figure 4. Unlike Conv-Net-SVM, Deep-SVM-Net has no dependence on convolutional layers and instead relies on stacks of dense layers to model higher-order feature interactions. The margin-maximizing classifier reduces the false-negatives with efficient inference, hence making it suitable for resource-constrained edge devices within IoMT infrastructures.

Chapter 2

RELATED WORK

Cybersecurity concerning IoMT domain has been seen considerable advances in recent times owing to the swift incorporation of smart medical devices, real-time systems for monitoring, and also connected hospitals. As indicated in Figure 1.1, IoMT encompasses different levels, including sensors at the device level, gateway controllers, cloud services, and clinical decisioning supports systems. The multiple levels involved make it possible to have different communication levels; hence, there is a need for intrusion detection mechanisms that can efficiently analyzes various kinds of traffics to detect any attacks accurately. Much has been also done concerning IDS in health-care settings, involving the development of IDS that employ rule-based approaches or hybrid deep learning models. This chapter offers an overview of significant advancements in IDS for IoMT, together with their pros and cons. The chapter outlines the research gap addressed by the proposed three deep learning IDS algorithms: Deep-SVM-Net, Conv-Net-SVM, and Embed-Net.

2.1 Traditional and Machine Learning-based IDS Approaches

Cybersecurity [8][9][12] in the fields of IoMT has been highly advanced in period of the past decade owing to fast growth in the use of medical devices, real-time system for monitoring, and IoT infrastructures in hospitals. There exist many layers in the IoMT system, which include devices' sensors, gateway controllers, cloud platforms, and clinical systems for decision-making, as shown in Figure 1.1. Since there are different types of attacks on multiple layers of the system, advanced intrusion detection mechanisms need to be designed to provide precise identification of malicious events. There have been a number of works related to the topic of intrusion detection in healthcare settings ranging from the classical IDS based on rule to deep hybrid learning-based systems. This chapter gives a brief overview of advances in the area, their pros, and cons and presents the research gap addressed by [28] three deep learning techniques: Deep-SVM-Net, Conv-Net-SVM, and Embed-Net.

Intrusion detection systems designed for detecting intrusions around medical environments, as well as those deployed in IoTs environments, heavily depended on signature-based

IDS methodologies, in which the network flow was matched against pre-defined rulesets. Signature-based IDS systems can detect known intrusions effectively; however, they are inflexible as well as ineffective in dealing with zero-day attacks and other kinds of attacks using new patterns. Dependence on static signature databases makes them less scalable, particularly in cases of rapidly changing medical environment traffic patterns.

Weaknesses in signature-based models which led to the incorporation of machine learning (ML) algorithms, including SVMs, Random Forest, Decision Tree, Logistic Regression, and KNN. These statistical models were able to perform anomaly detection by capturing the network traffic anomalies. Several early studies made use of SVM-based classifier algorithm on various benchmarks like KDD99, UNSWNB15, and NSL-KDD in order to detect DoS, probes, and U2R attacks with moderate levels of detection precision. Ensembles like AdaBoost, Gradient Boosting, and Random Forest algorithms showed superiority in terms of detecting intrusions with reduced risk of overfitting.

However, most of the ML-based IDS frameworks still suffered from inherent limitations when applied to IoMT environments. First, the feature space in medical network data is very heterogeneous, as it combines numerical flow statistics with symbolic categorical attributes like authentication flags, protocol identifiers, device types, and port level sequences. Most classical machine learning algorithms rely on handcrafted feature engineering and are sensitive to class imbalance and nonlinear complex attack pattern generalization. Besides, most of the IoMT devices operate under very constrained computational resources, making many ML pipelines impracticable for on-device or near real-time detection. These challenges motivated the exploration of deep learning architectures capable of end-to-end feature extraction.

2.2 Deep Learning Approaches to IoMT Intrusion Detection

Deep learning emerged as a strong alternative, able to automatically identify meaningful patterns from minimally preprocessed data. CNN, RNN, AE, and hybrid deep learning architectures report remarkable enhancement in accuracy and generalization performance for intrusion detection. Some CNN-based IDS models extracted remarkable discriminatory features by identifying spatial correlations within the traffic flows. In particular, LSTM and GRU [1] networks model temporal dependencies that arise among the sequential attack behaviors. Variants of autoencoders, such as SDAE-based IDS, utilize the reconstruction

error to identify anomalies, which was found to be effective in unsupervised learning and the identification of rare patterns. Despite these advantages, deep learning systems have brought new challenges. Most of these architectures require heavy computational resources and large training datasets, hence deployment on lightweight IoMT devices is infeasible. Although autoencoder-based methods performed well for anomaly detection, they often incurred longer training times and were susceptible to noise in traffic data. CNN IDS models performed well when structural patterns were meaningful but struggled to process mixed categorical and numerical attributes without inflating dimensions through one-hot encoding. Sparse and very high dimensional representation further slowed down inference and usage of memory. Such problems also led to the development of DL-models, that could process the heterogeneous data features in medical networks efficiently without a very large increase in computational cost.

These include embedding models, CNN-SVM models, and margin based deep neural networks (DNN). The above-mentioned models constitute the basis for the three models to be compared in this study, namely, Embed-Net, Conv-Net-SVM, and Deep-SVM-Net whose architectural diagram is shown in Fig. 3.3, Fig. 3.4, and Fig. 3.5, respectively.

2.3 Challenges in Developing IDS for IoMT Environments

Despite the considerable progress made in this field during the past several years, designing an efficient IDS architecture for IoMT networks is still a quite challenging task. While corporate environments do not involve many heterogeneous devices, IoMT systems require to operate a wide range of diverse components, which include various medical devices, wearables, cloud-based platforms, embedded gateway modules, and infrastructure for real-time communication. The above-mentioned properties of IoMT systems impose a number of limitations that affect intrusion detection capabilities.

The first major challenge associated with IoMT systems is caused by their constrained nature. Many portable medical devices are characterized by low energy consumption, modest computing capabilities, and limited memory storage capacity. For this reason, using standard approaches and techniques for security purposes may become problematic. In particular, applying computationally complex algorithms based on neural network architectures seems inappropriate for lightweight IoMT devices.

The other important problem in relation to IoMT is the high heterogeneity of data. IoMT

traffic data consists of both numeric continuous features and discrete categories of traffic elements, like device ID, communication protocol, authentication mode, service ports, and connection status. Traditional ML algorithms usually have difficulties with handling such types of data, particularly when it comes to categorical features encoding through sparse one-hot encoding. It causes higher computational costs and decreased efficiency of inference in terms of accuracy.

Class imbalances are quite common in IoMT applications. In healthcare networks, regular benign traffic significantly exceeds malicious traffic, which may happen occasionally. As a result, it causes an underestimation of the minority attacks' classes and makes intrusion detection models focus mostly on majority samples. The situation is especially hazardous in the context of IoMT, as any attack will put patients' health at risk and disrupt healthcare provision in emergencies.

The other obstacle associated with detecting attacks relates to the ever-changing nature of cyber threats. The attackers regularly adapt their methods of penetration, create zero-day vulnerabilities and exploit them, and form advanced patterns of cyberattacks that allow them to overcome traditional signature-based models of IDS functioning. Static IDS systems based solely on the recognition of signatures of previous attacks cannot detect new types of attacks. Thus, contemporary IDS designs should be endowed with advanced learning abilities as well as good generalization properties.

Additionally, the need for privacy and confidentiality imposes another constraint on the problem under consideration. IoMT systems regularly work with highly sensitive medical information, comprising patients' physiological parameters, diagnoses, clinical records, medical histories, and so on. Therefore, any breach of the confidentiality of medical data will entail legal problems as well as loss of public confidence.

Immediate reaction is also one of the key requirements in health care infrastructures. The delay in identifying an intrusion can cause severe damage, particularly in critical environments, like ICUs, remote surgery stations, and systems that constantly monitor patients. It is important that intrusion detection systems used in these settings should be able to provide immediate threat identification while sustaining their efficiency levels in a constant stream of data.

All these factors indicate that the IoMT-based intrusion detection needs to go beyond traditional security approaches. In particular, intelligent deep learning models tuned to work with heterogeneous medical traffic and unbalanced attacks under limited resources need to

be employed.

2.4 Importance of Dataset Quality in IoMT Intrusion Detection

The success of an IDS relies heavily on the quality of the data set that was used for training and testing. It is especially true when talking about IoMT cybersecurity research due to the fact that traffic within healthcare differs greatly from traditional business and industrial settings. Medical communication patterns involve continuous sensor transmission, emergency-triggered events, periodic monitoring flows, and interactions among heterogeneous healthcare devices, all of which must be properly represented in the training data.

The past intrusion detection studies mainly utilized benchmark datasets like KDD99 and NSL-KDD. Even though the use of these benchmark datasets has been very significant in the advancement of IDS research, these datasets have since proven inadequate for the present day IoMT environment. Most of the datasets used in the past consist of outdated traffic behavior, impractical attacks, and unrealistic communication structures that do not represent today's healthcare infrastructure well enough.

Unlike the past intrusion datasets, the contemporary IoMT datasets try to overcome these limitations by adding realistic healthcare traffic and attacks. The contemporary IoMT datasets, such as ECU-IoHT, WUSTL-EHMS, NF-BoT-IoT, and CICIDS2017, consist of various types of attacks ranging from distributed denial-of-service attacks to reconnaissance, spoofing, ransomware, and even botnet communications. In addition to that, these datasets consist of realistic network flows captured from smart healthcare, IoT gateways, and wearables.

Nevertheless, there are certain limitations that can be observed in current IoMT datasets. One of them is related to the balance of data in a dataset since the ratio of benign traffic samples exceeds the number of malicious traffic samples. Models created using the imbalanced IoMT dataset will be biased towards normal behavior, making it difficult for the model to detect anomalies.

Also, there is no consistency between various datasets used in IoT security. In other words, IoMT datasets may vary in traffic forms, attack types, feature extraction approaches, and so on. As a result, comparison becomes a problematic task. Thus, the high-performance of an intrusion detection model created based on one IoMT dataset does not guarantee the

same results when testing another healthcare system.

It is also imperative that there should be some form of dataset diversity so as to increase the robustness of intrusion detection models developed. There are various different kinds of devices, protocols, and situations in actual health care network scenarios. Datasets that have limited attacks and limited interaction of various devices can result into overfitting, whereby models end up learning from the datasets, instead of the nature of intrusions.

There have been several research studies conducted that have focused on increasing dataset diversity, by adding health care network traffic in real time, distributed attack simulation, and diverse communication between devices. Researches have also used artificial dataset generation methods such as SMOTE and adversarial learning.

Therefore, it is critical to note that selection of relevant datasets is a basic prerequisite in IoMT Intrusion Detection research. The use of good quality datasets increases the performance of IDSs while also contributing to making functional systems.

2.5 Prior Research on IoMT Intrusion Detection

Kabir et al. (2018) used a novel LS-SVM-based [1] IDS model on the KDD99 dataset. In this work, the authors made use of a dual stage algorithm for decision making, to improve the reliability of the detection process. The authors managed to reduce the computational cost while still retaining strong predictive power with an accuracy of 97.64%, a recall of 90.89% and F1-score of 94.14%.

Aldwairi et al. (2018) analyzed Restricted Boltzmann Machine (RBM) through the application of ISCX dataset. It should be noted that RBM has a unique advantage of being able to identify and adapt to any previously unseen pattern. Using RBM, the authors reported a detection accuracy of 84.7% with an accuracy of 79.8%.

Aljawarneh et al. (2018) designed and implemented a hybrid machine learning system using Naïve Bayes, AdaBoostM1, J48, REPTree, and RandomTree on the NSL-KDD dataset. The research focused on the feature selection process, more specifically, through information gain technique. This hybrid achieved an accuracy of 99.81%; however, it has a higher rate of false negatives, hence less suitable for IoMT applications in real-world critical scenarios.

Abusitta et al. (2019) proposed an SDAE-IDS, which was evaluated on the KDD Cup 99 dataset. The detection of intrusion in cloud-based IoT and IoMT environments using deep

reconstruction learning was the aim. The model gave an accuracy of 89.2%, proving more robust than the baseline methods but at higher computation costs.

Gu et al. (2019) proposed the DT-EnSVM method, which was tested on NSL-KDD, Kyoto2006+, and KDD99 datasets, by integrating decision trees with margin-based classification via SVMs. The results revealed that their ensemble achieved 99.41% accuracy, 99.09% detection rate, and a 0.31% false-alarm rate, with good generalization on different datasets.

Kim and Park (2019)[6] proposed a reinforcement-learning-driven model, DAEQ-N, integrating Deep Autoencoder and Q-Learning, and evaluated it on the KDD99 dataset. The approach uses reinforcement signals to dynamically adjust detection behavior for changing network environments, yielding high detection capability at the cost of high computation.

Zhou et al. (2020) proposed a feature selection and ensemble framework using Correlation Feature Selection (CFS) with the [7]Bat Optimization Algorithm (BA), evaluated on NSL-KDD, AWID, and CIC-IDS2017. The model achieved an accuracy close to 99.89%, validating the efficiency of hybrid feature optimization.

Li et. al. (2020) created an Autoencoder-based Intrusion-Detection-System (IDS) optimized with Random Forest by using the CSE-CIC-IDS[8]2018 data. The model combined deep reconstruction learning with tree-based classification and achieved strong detection performance, though the autoencoder introduced higher training overhead.

Zhou et al. (2020) [9]also proposed M-AdaBoost-A, an optimized boosting ensemble evaluated on AWID and NSL-KDD datasets. The approach iteratively reweighted misclassified samples and achieved 99.99% accuracy, but with increased processing time due to multiple boosting iterations.

R.M. et al. (2020) proposed PCA-GWO-DNN, combining Principal Component Analysis, [10] Grey Wolf Optimization, and Deep Neural Networks, tested on the Kaggle IoT dataset. It simplified feature reduction while improving training efficiency and reached an accuracy of 99.9% with 95.4% recall, demonstrating strong multi-class IoT attack detection.

Ahmed et al. (2021) introduced an IoMT-specific dataset called ECU-IoHT [11] and presented baseline IDS evaluation using KNN-based methods. Their primary contribution was dataset creation rather than model architecture, enabling realistic benchmarking for IoMT-centric IDS evaluation.

Shahzad et al. (2021) presented a Two-Step Ontological Model for semantic reasoning and interoperability in IoT-based healthcare. Although not a traditional IDS model, it

supported [12] knowledge-driven decision support and threat awareness.

Alazab et al. (2022) deployed the Moth-Flame Optimization algorithm with a [13] Decision Tree classifier on KDD99, NSL-KDD, and UNSW-NB15 datasets. Their optimized feature selection improved detection performance, achieving 97.8% accuracy and a 99% F1-score, although the model was sensitive to hyperparameters.

Qazi et al. (2022) proposed a stacked non-linear denoising autoencoder followed by an [14] SVM classifier on the KDD Cup 99 dataset. Their model achieved 99.65% accuracy, 99.99% precision, and 99.85% recall, but required expensive deep training cycles and regularization.

Patil et al. (2022) presented a [15] LightGBM + LIME explainability framework on CICIDS-2017, focusing on interpretability. The model achieved 96.25% accuracy, trading off peak performance for explainability.

Firat Kilincer et al.[16] (2023) performed Recursive Feature Elimination with MLP/XGBoost on ECU-IoHT, TON-IoT, and WUSTL-EHMS datasets, improving feature selection and achieving near-perfect 99.99% accuracy, although computation complexity increased.

Mosaiyebzadeh et al. (2023) proposed a Federated Learning + DNN-based IDS for the [17] ECU-IoHT dataset to enable privacy-preserving distributed learning. Although data confidentiality improved, communication overhead limited scalability.

Thulasi and Sivamohan (2023) proposed [18] MSCSL, a hybrid Multi-Step CNN + Stacked LSTM model tested with ECU-IoHT and several other IoT datasets. The model achieved 98.95% accuracy with strong temporal and spatial learning but caused higher computational delays.

Azimjonov and Kim (2024) proposed a lightweight IDS using a [19] fine-tuned SGD classifier on BotIoT, N-BaIoT, and KDD99[19] datasets. Their model emphasized fast computation and low memory usage but delivered lower accuracy (92%) for minority attack classes.

Zhang et al. (2024) employed MIC-XGBoost by combining maximum information coefficient filtering with tree-based boosting on [20] WUSTL-EHMS, CICIDS2017, and ECU-IoHT datasets. The model achieved 95% accuracy but struggled to generalize across datasets.

Nazir et al. (2024) introduced a hybrid [21] CNN–LSTM with 99% accuracy, demonstrating strong temporal-spatial learning capacity but requiring higher computational resources.

Aguru and Erukala 2024 proposed SM-GRU [22][23], which integrated the spatial map-

ping mechanism with GRU layers, while attaining a high F1-score of 98.56%. Although effective, this approach incurred extended processing times.

Saheed et al. 2024 proposed GA-LSTM [24], which incorporates genetic algorithm optimization into the LSTM. This design gave an accuracy of 99.41%, but the sequential process of learning introduced latency in inference.

Chintapalli et al. (2024) proposed an Osprey-Optimized Bi-LSTM [25] that achieved 99.98% accuracy on the CICIDS-2017 and N-BaIoT datasets. While the model provides state-of-the-art detection, it suffers from extremely high computational overhead that is infeasible for low-power IoMT systems.

While the earlier approaches, such as LS-SVM and RBM-based IDS, had demonstrated moderate accuracy on KDD99, NSL-KDD, and ISCX benchmarks, they did have drawbacks, such as being very expensive computationally, limited scalability, and poor adaptability to unseen attack variations. Autoencoder-based models represent deep representation learning for intrusion detection, including SDAE-IDS, AE-IDS, and S-NDAE-SVM, which obtained remarkable detection accuracy; however, they involved considerable GPU computation and thus are infeasible for real-time IoMT inference.

The MFO-DT, PCA-GWO-DNN, RFE-MLP, and evolutionary deep learning models demonstrated effective feature selection and outperformed many others in terms of classification for many datasets like CIC-IDS 2017, UNSW-NB15, AWID, and ECU-IoHT. Indeed, many of these models reported detection performances well over 99% for controlled experimental conditions. However, their runtime complexities, dependency on meta-heuristic tuning, and expensive inference hinder their feasibility for actual deployment in medical devices.

Hybrid architectures included CNN-LSTM, Bi-LSTM with evolutionary tuning, and SM-GRU, which integrated sequential learning with strong temporal modeling capabilities. While demonstrating high detection performance, these models had substantial latency and runtime overhead because of their sequential designs, hence limiting their applicability in time-critical medical environments.

Lightweight IDS models, represented by variants of SGDC, MIC-XGBoost, and kNN, offered reduced latency and faster inference but generally sacrificed accuracy, particularly for rare attack classes. However, these algorithms fail miserably in the recognition of minority cases of intrusions-an inherent problem in cybersecurity for the healthcare industry because a false negative could mean real-life implications for patients. On the other hand,

the healthcare-specific attacks like those in the ECU-IoHT dataset added realism to the test cases for intrusion detection in the IoMT industry. Nevertheless, most of the recent IDS models still have one or more of the following issues:

- Very high computational expenses is often linked to higher accuracy, which makes it bad for IoMT devices.
- Available models poorly deal with categorical network attributes common within medical traffic.
- Imbalanced data sets severely degrade detection accuracy for all minority attack classes.
- False-negative reduction remains an unknown study topic and poses severe risks to healthcare safety.

These limitations that justify the need for advanced architecture such as Embed-Net, Conv-Net-SVM, and Deep-SVM-Net.

Chapter 3

METHODOLOGY

The paper focuses on the systematic development, training, and validation of three deep-learning models, namely, Embed-Net, Conv-Net-SVM, and Deep-SVM-Net, for intrusion detection in the IoMT. Each model has been selected based on different architectural characteristics and their merits to overcome the shortcomings of traditional IDS. The proposed methodology unifies dataset preprocessing, feature engineering, model construction, training configurations, and evaluation procedures in a single framework. This chapter explains the flow from the beginning with the pre-processing of data up to model inference, for conceptual references to Figures 3.3, 3.4 and 3.5.

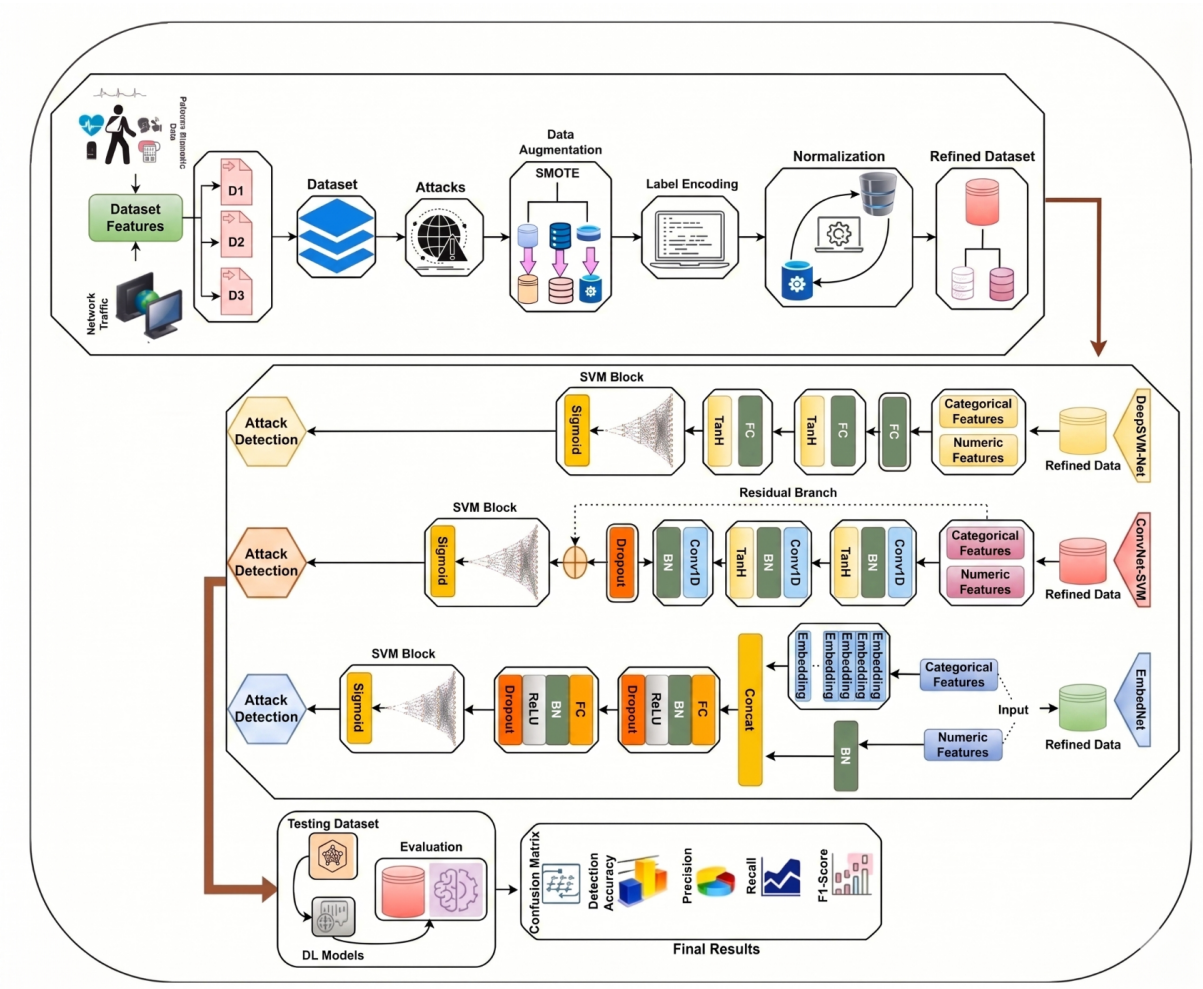


Figure 3.1: Overall the workflow of the proposed IoMT intrusion detection framework integrating preprocessing, DL architectures, and also evaluation stages.

3.1 Data Preparation and Preprocessing Pipeline

IoMT network traffic is composed of packet metadata that describe the communication protocols, device interaction patterns, flow-level statistics, packet directionality, and a lot of flag indicators. In order to effectively train deep-learning architectures, these features need to be transformed into structured numerical inputs through an elaborately designed preprocessing sequence.

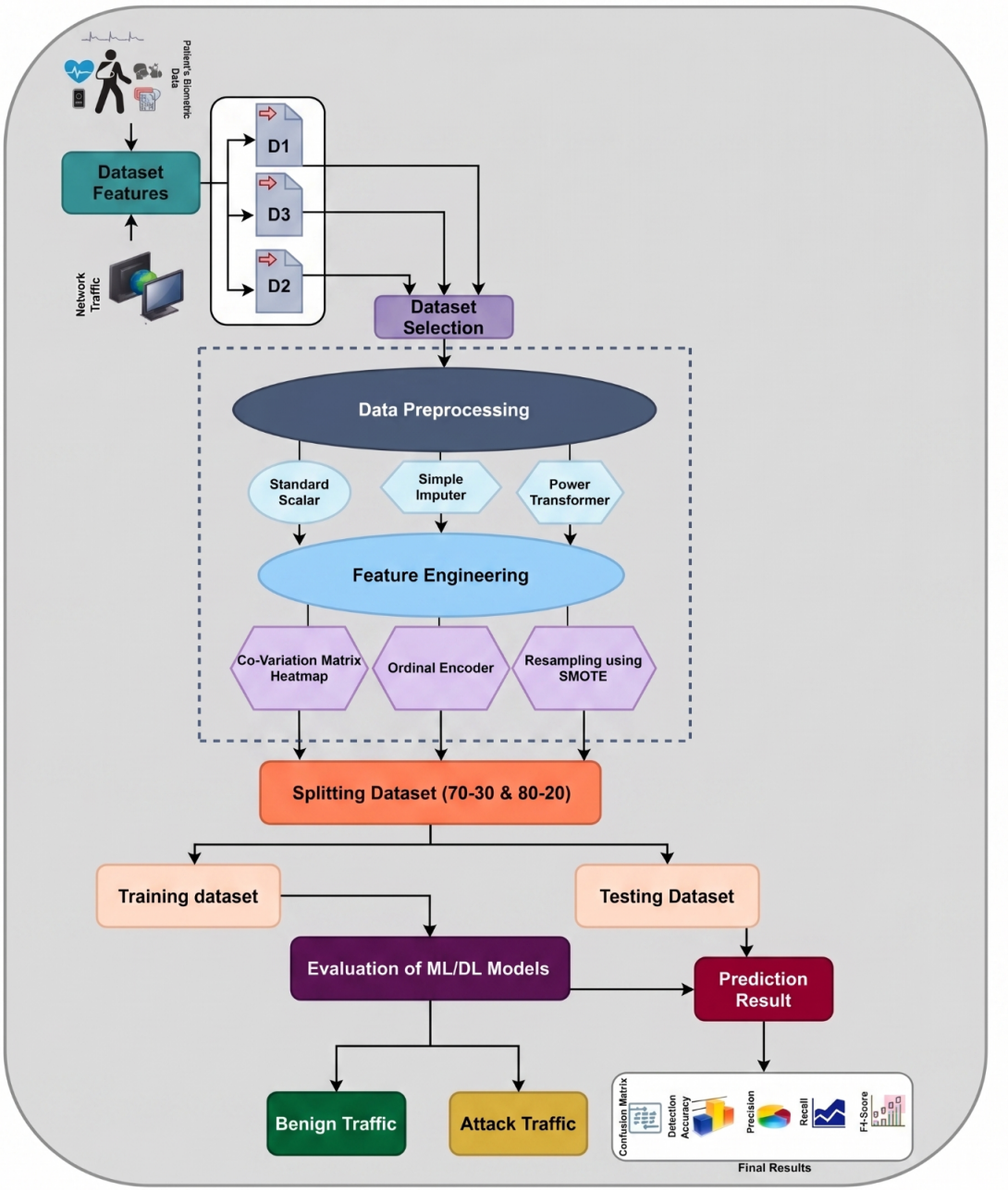


Figure 3.2: Lab experimental flow for proposed framework for attack detection in IoMT networks.

3.1.1 Cleaning the Dataset and Removing Redundancy

The preprocessing pipeline starts by removing attributes that are redundant and add limited discriminative power. It then performs covariance analysis in order to find strongly correlated features. An example of excising repetitive MAC addresses, IP fields, or direction indicators also helps to remove noise or duplicate semantic content. Figure 1.1 illustrates the layered IoMT data flows that require a structured approach for proper representation.

3.1.2 Missing Value Imputation

Missing numerical and categorical attribute values are imputed to maintain statistical consistency in model training:

- Imputation of mean or median values for continuous numerical fields
- Mode-based imputation for the categorical-variables

Categorical variables - imputation based on mode Such preprocessing prevents instability during optimization and preserves the characteristics of the traffic distribution.

3.1.3 Encoding of Categorical Features

IoMT datasets typically include categorical attributes such as:

- Protocol Type
- Device Identifiers
- Connection Flags
- Service Types

Instead of traditional one-hot encoding—which would dramatically increase dimensionality—ordinal encoding is applied to convert symbolic fields into integer indices. These encodings are subsequently embedded through the categorical embedding layers of Embed-Net (Figure 3.3) and processed as indexed features in Conv-Net-SVM and Deep-SVM-Net.

3.1.4 Normalization and Transformation of Numerical Attributes

Continuous features are normalized in two stages:

- Standard Scaling to achieve zero mean and unit variance
- Power Transformation to reduce skewness in non-Gaussian traffic distributions

This transformation improves stability of gradient propagation and enables smoother convergence across all three models.

3.1.5 Handling Class Imbalance Using SMOTE

IoMT datasets suffer from severe class imbalance, as benign traffic dominates while malicious flows are sparse. To mitigate this imbalance, the SMOTE oversampling strategy generates synthetic minority-class samples by interpolating between nearest neighbors. This steps significantly enhance the detection of the rare attacks and also reduces false negatives.

3.1.6 Data-set Splitting & Cross-Validation

The datasets are partitioned into training and testing components using an 80 is to 20 splits. To evaluates robustness and also prevent overfitting, 10-fold cross-validation are adopted. The multi-stages validation ensures:

- Reliable performance estimation
- Reduced variance due to random splits
- Fair comparison across all three architectures

3.2 Architecture of Proposed Models

The proposed three deep-learning models—Embed-Net, Conv-Net-SVM, and Deep-SVM-Net—are depicted in Figures 3.3, 3.4, and 3.5. Although fundamentally different in design, they share the same goal of accurate, real-time IoMT intrusion detection.

3.2.1 Embed-Net: Embedding-Based Deep Learning Architecture

Embed-Net is specifically constructed to handle heterogeneous IoMT data. Unlike traditional neural networks that treat each categorical feature as a discrete token, Embed-Net learns dense categorical embeddings that capture semantic similarity among protocol types, services, authentication flags, and device identifiers.

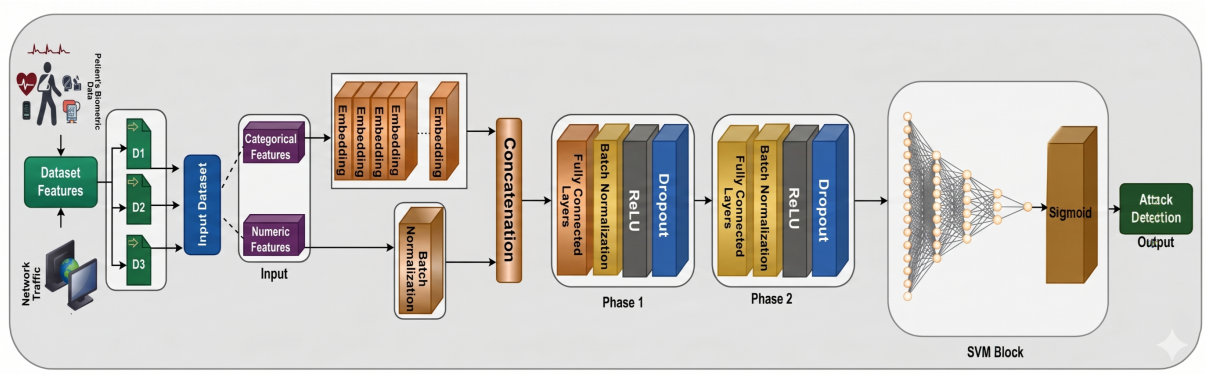


Figure 3.3: Working architecture of Embed-Net model.

Embed-Net is developed to address the specific challenges of heterogeneous IoMT data that have a rich mixture of categorical, numerical, and protocol-level attributes. Traditional deep learning architectures take the categorical values representing protocol types or flag indicators as separate tokens and represent them using very sparse one-hot vectors. This leads to the problems of ultra-high-dimensional inputs and loss of meaningful relationships among categories. Embed-Net learns compact, dense categorical embedding vectors so that the model can capture subtle semantic similarities among symbolic IoMT attributes.

This embedding mechanism allows the network to treat the symbolic attributes uniformly in a conceptual way, similar to natural language tokens: all are assigned vector representations that develop during training. As an example, the model may learn that TCP and UDP behave more similarly than ARP broadcasts, or that SYN–ACK sequences resemble each other more strongly than RST packets. This level of representation learning is very important for intrusion detection, where even small categorical variations might represent early attack behavior.

3.2.1.1 Architectural Workflow

- **Categorical Embedding Layer:** Here, each symbolics attribute like (protocol, service, etc.) is mapped into an embedding vector of dimension 8–16, representing se-

mantics structure across the categories.

- **Normalization of Continuous Inputs:** Here numerical features like packet duration, byte counts, and flow statistics are then batch-normalized to stabilizes optimization.
- **Concatenation Layer:** Here embedded categorical vectors are been concatenated with normalized continuous features to produces a unified inputs vector.
- **Deep Fully Connected Layers:** Here, unified vector are passes through multi-layer of dense transformations with dropout and then nonlinear activation.
- **Classification Layer:** Here A sigmoid classifier produces the probability score of malicious activities.

3.2.2 Conv-Net-SVM: Hybrid Convolution + Margin Classifier

Conv-Net-SVM combines convolutional feature learning with SVM-based margin separation. CNN layers detect structural and spatial correlations in traffic patterns—useful for identifying DDoS bursts, port scans, and probing sequences—while the SVM layer enforces a large-margin separation between benign and malicious classes.

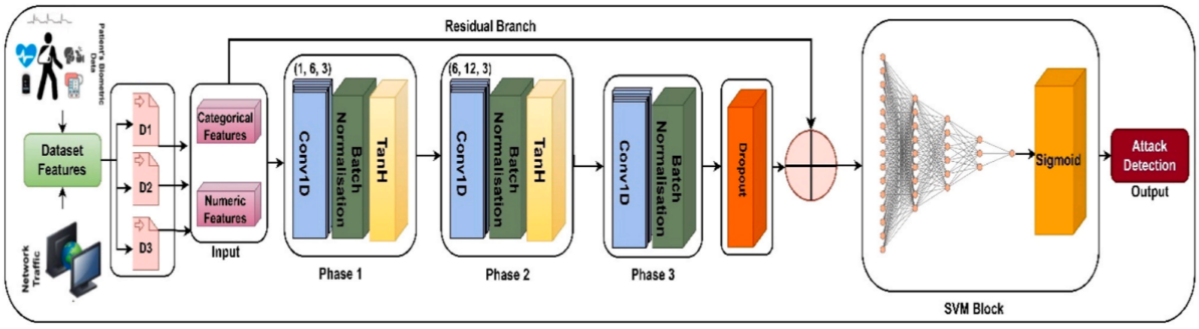


Figure 3.4: Working architecture of Conv-Net-SVM model.

By design, Conv-Net-SVM is a hybrid model that combines the complementary strengths of CNNs with the robust decision-margin characteristics possessed by SVMs. Unlike Embed-Net, which focuses on embedding categorical features, Conv-Net-SVM analyzes IoMT traffic patterns through convolutional filters sliding along feature vectors in search of local structural correlations. These convolutional filters behave like feature detectors that are able to recognize repeated or abnormal sequences within network traffic flows, which is highly advantageous for identifying volumetric attacks such as DDoS, probing attempts, or sequential scanning behavior.

Traffic features are transformed into a structured 1-D or 2-D representation to which convolution filters can learn to recognize patterns across adjacent features. For example, in 1-D convolution, the filters might learn to recognize anomalies in packet size progression, byte distribution, or flag transitions. Alternatively, in the 2-D convolutional variants, flow statistics can be laid out spatially to mimic image-like feature maps that can be analyzed by more sophisticated local pattern recognition.

The hierarchical feature maps are generated by CNN layers. Typically, the first convolution layer learns low-level attributes such as sudden spikes in packet count, while deeper layers learn abstract behaviors such as sustained abnormal flow bursts or distinctive IoMT device misuse patterns. These are typically complemented by pooling layers that reduce spatial dimensionality, suppress noise, and focus only on the most discriminative feature activations.

Batch Normalization ensures stable gradient flow by normalizing the intermediate feature maps. Therefore, the network becomes independent of the initial values and learning rates that are chosen by us. After the spatial patterns have been separated using discriminative learning, the next step involves conversion of these features into a 1-D vector through the process of flattening.

The unique aspect about the Conv-Net-SVM architecture when compared to other conventional CNN models lies in its final classifier. Unlike other classifiers, it uses a Support Vector Machine function as the final classification step. Margin maximization is one of the main benefits offered by the SVM model. This enhances generalization and significantly reduces misclassification within IoMT traffic distributions that are mostly overlapping or noisy. Conv-Net-SVM is particularly effective for the attacks with the temporal, wave-like, or the sequential patterns, such as the port scans or the botnet command bursts. While heavier in terms of computations due to the convolutional operations, the structural learning capability gives it a competitive edge within environments that have patterned attacks.

3.2.2.1 Architectural Workflow

- **Reshaping of Numerical Attributes:** Numerical and encoded features are structured into 1-D or 2-D grids suitable for convolution.
- **Convolutional Feature Extraction:** Convolutional filters detect spikes, waveforms, and structural attack signatures.

- **Pooling and Batch Normalization:** Pooling layers reduce feature noise and dimensionality, while normalization stabilizes activation statistics.
- **Flattening:** Multi-dimensional feature maps are flattened into a dense vector.
- **SVM Classification Layer:** Instead of a softmax classifier, a margin-based SVM layer is used to minimize misclassification error.

3.2.3 Deep-SVM-Net: Deep Neural Network with Margin-Based Classification

Deep-SVM-Net replaces convolutions with fully connected layers while maintaining a margin-inspired classifier.

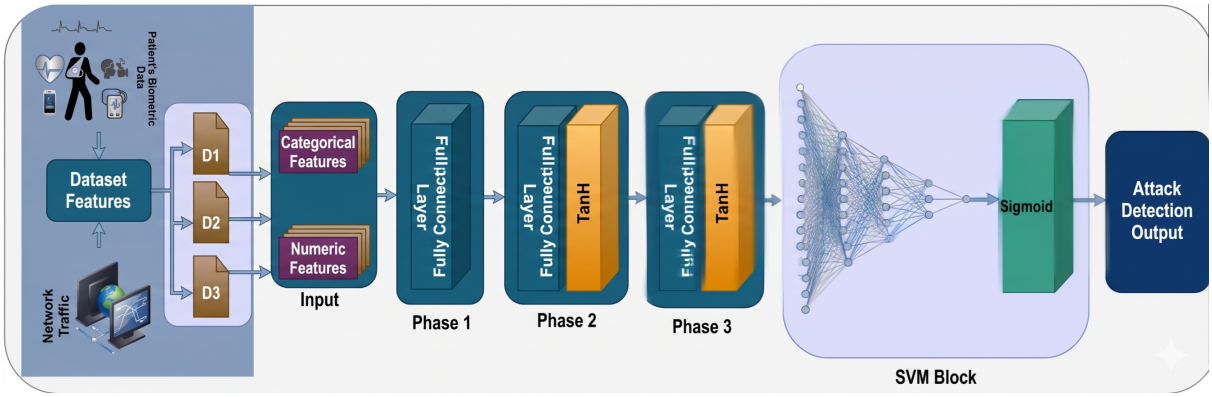


Figure 3.5: Working architecture of Deep-SVM-Net model.

Deep-SVM-Net is an innovative lean-but-powerful deep learning model designed to extract nonlinear IoMT data features with the help of fully connected layers while introducing the margin-based decision-making spirit of SVM right at the output. Unlike Conv-Net-SVM, Deep-SVM-Net avoids using convolution, making it faster and hardware-friendlier-a critical aspect for resource-constrained IoMT devices.

IoMT data can also be noisy or exhibit feature overlapping traffic patterns; hence, a margin-based classifier adds more robustness and reduces false negatives. Moreover, Deep-SVM-Net has a much lighter architecture than many of the CNN-based models, so it fits well on fog nodes, medical wearables, and embedded IoMT gateways that require fast inference on limited compute power.

3.2.3.1 Architectural Workflow

- **Dense Feature Extraction Layers:** Multiple dense layers extract latent traffic representations.
- **Batch Normalization and Dropout:** Here, reduces overfitting and also stabilize gradient learning.
- **Margin-Based Output Layer:** Here, replaces softmax with an SVM-like margin objective, the improving separation between benign and also malicious samples.
- Epochs: 100
- Batch sizes: 64, 128, 256
- Optimizer: Adam
- Learning rate: 0.0001
- Loss functions:
  - Binary cross-entropy for Embed-Net and Conv-Net-SVM
  - Margin-based loss for Deep-SVM-Net

3.2.4 Regularization Techniques

The methods that help generalize and prevent overfitting, key considerations in IDS where new attacks have to be identified, include: - Dropout: The model is forced into distributing its learning by randomly turning off neurons.

- Batch Normalization: This method helps stabilize the activation process, accelerate convergence, and also increase robustness.

- Early Stopping: Training is stopped when there is no further gain or even deterioration in validation loss.

- Dropout layers reduce overfitting
- Batch Normalization is stabilizes in training dynamics
- The early stopping monitors the validation loss to prevent the excessive training

3.2.5 Cross-Dataset Generalization

The models have been analyzed using different benchmarking datasets of the IoT to make sure that they provide a good generalization capability in the face of different types of networks. All three models are analyzed by the use of different IoMT datasets:- ECU-IoHT, WUSTL-HDRL-2024 NF-BoT-IoT which prove their capability to generalize in a different environment.

3.3 Feature Engineering and Dimensional Optimization

The importance of the selected feature extraction algorithm cannot be underestimated due to the fact that the quality of the chosen characteristics can have an effect on the ability of the deep architecture to learn from the input information. The IoMT network traffic data usually comprises numerous features that relate to the statistical properties of packets, communication behavior, protocol information, temporal aspects, as well as interaction characteristics for devices. However, some of them are not essential for the attack identification.

In order to deal with this problem, a special feature engineering approach is applied to the developed methodology. At the very first stage, irrelevant features are eliminated, namely those with too much missing data, constant value distributions, as well as duplicate meanings.

Additionally, correlation analysis is utilized in identifying numerical attributes that demonstrate a very high level of dependency. The attributes that show very high covariance or similar statistical behaviors are excluded to reduce redundancy and decrease the dimensions of feature space. The removal of such attributes does not affect the detection process in a significant way.

Categorical attributes, however, are not directly represented through one-hot encoding, as it produces very large and sparse feature spaces. Instead, categorical attributes are represented using integer-based encoding, which facilitates embedding-based learning. This technique can be particularly helpful for IoMT devices, as protocol identifiers, services types, and communication flags tend to consist of a great deal of symbolic values.

In addition, another critical point about feature engineering is that it is essential to maintain behavioral characteristics that can be exploited by an attack within the new feature space created by the transformation. Feature characteristics involving packet rate, unusual communication bursts, connection length, byte transfer rate, and failed logins are maintained

since these may give critical indications of malicious attacks.

Feature engineering is not only geared towards better accuracy but also towards more efficient processing. Lower dimensionality reduces memory utilization and increases optimization speed, making deployment easier and more feasible in real-world IoMT scenarios. Hence, optimization greatly assists in achieving a more robust and scalable framework for intrusion detection.

3.4 Training Strategy and Model Optimization

The efficiency of deep learning architectures greatly relies on the quality of training technique used in the process of building a model. Within intrusion detection systems, any misadjustment in optimization techniques can cause unstable convergence, overfitting, or inadequate generalization to unseen attack instances. Hence, a well-designed training approach has been applied in ensuring the reliable performance of IoMT intrusion detection models.

The mini-batch optimization has been adopted for training all the three models of deep learning architectures to ensure gradient stability and speed of convergence. Different mini-batch sizes are tested in terms of their impacts on learning dynamics, memory requirements, and model stability. Mini-batch sizes that provide noisy yet adaptable gradient updates usually perform better than those with smooth yet fast performance.

Adam optimization method is used for training parameters due to its adaptiveness and convergence nature. Adam algorithm incorporates the momentum and the adaptive rate adjustment in order to facilitate effective convergence of the models under consideration, considering that the IoMT traffic can be highly heterogeneous.

Furthermore, batch normalization technique is added to the suggested architecture in order to provide greater training stability. The application of the batch normalization facilitates faster convergence, stable gradient flow, and reduces the dependence on initial weight values.

Finally, the regularization technique based on dropout is applied in order to prevent the issue of overfitting. Dropout is used to randomly drop a part of the neurons during each iteration of the training phase in order to force the model to learn general features that will help detect new attacks.

Early stopping techniques are also used to avoid overtraining. The validation loss func-

tion is continuously monitored during the training stage, and the training optimization is halted when no more improvements can be seen on the model's performance through consecutive epochs. This helps avoid memorization of the training data and ensures good performance on unknown IoMT traffic.

Finally, hyperparameter tuning is carried out through experiments to ensure that the learning rate, the dropout probability value, the number of nodes in the hidden layers, the batch sizes, and the number of epochs result in a stable system configuration.

The training methodology described is geared towards building a system that will guarantee high performance levels and computational feasibility in IoMT-based healthcare environments.

3.5 Real-Time Deployment Considerations for IoMT IDS

Although accuracy is an important attribute to strive for in an IDS, the actual feasibility of deploying any detection scheme within an IoMT infrastructure should not be ignored. Infrastructures used in healthcare require continuous and real-time data exchange among wearable IoT devices, smart sensors, controllers, and even healthcare applications stored in the cloud. Thus, any ID framework designed for this scenario should meet certain conditions regarding latency, computation load, power consumption, and reliability.

The first major difficulty that arises from this situation lies in the limited capabilities of the medical hardware used in IoT infrastructures. Since most of the IoT components are embedded devices, their capabilities are lower than those of traditional computers. As a result, deep neural networks that utilize very powerful computing capacity might prove to be unusable on such devices directly.

The Embed-Net model is particularly applicable to environments where there is need for rich feature representation and accurate detection of threats. The model's embedding approach allows efficient processing of heterogeneous categorical variables while ensuring relatively low memory consumption. As such, it can be used in hospital gateways, edge servers, and cloud-based healthcare systems.

Conv-Net-SVM, despite its excellent performance in detecting structural attack patterns, incurs relatively high computational costs. In view of the above, the model's deployment would be most suited in high-computational power fog nodes or special healthcare security servers.

Deep-SVM-Net is ideal for scenarios where light deployment of models is required. Owing to its avoidance of costly convolution and the use of dense feature representation, Deep-SVM-Net offers relatively fast computation and reduced memory consumption. Thus, the model would be best applied in portable healthcare devices, embedded hospital gateways, and wearables.

A further aspect to consider relates to the latency of inference processing. In the context of healthcare, any delay in detection might interfere with emergency communication, diagnostics or even patient care. Thus, one of the key aspects of the developed intrusion detection approach is the ability to perform inference in a fast manner without compromising classification accuracy.

The scalability issue should also be mentioned when deploying the developed framework in practice. Nowadays, there can be thousands of medical devices connected in a single healthcare system which will constantly produce network traffic. The developed methodology allows scalable deployment by using flexible preprocessing pipelines and efficient machine learning architectures suitable for processing massive amounts of traffic data.

Such considerations guarantee that the proposed approach is both feasible and effective.

Chapter 4

RESULTS AND DISCUSSION

The performance evaluation of the three proposed deep learning (DL) models are for intrusion detection in IoMT environments: Embed-Net, Conv-Net-SVM, and Deep-SVM-Net. The measures used in evaluating performance include accuracy, stability of learning process, generalization ability, false negative tendencies, and computational complexity. The explanations of the outcomes presented are made on the basis of the training/validation graphs in Figures 4.1 to 4.2. The graphs show how each architecture behaves under various training conditions and the components within it that contribute to improved performance.

4.1 Evaluation Metrics and Experimental Setup

The performance metrics used to evaluate the performance of the proposed IDS models are:

- **Accuracy:** The overall percentage of samples that were successfully classified.
- **Precision:** The capacity to appropriately identify harmful instances in order to prevent false alerts.
- **Recall:** The capacity to successfully identify real harmful activity.
- **False Negative Rate (FNR):** The frequency at which attacks are mistakenly classed as normal is known as the False Negative Rate (FNR). For the IoMT applications, where the undetected breaches could be directly jeopardize patient care, this metric is the especially important.
- **Training/Validation Loss:** Here, it shows how well the model are generalizes to new samples and also fits the training set.
- **Computational Efficiency:** Here, it is Suitability for the real-time IoMT deployment with respect to the resource use and also inference time.

4.2 Embed-Net: Results and Interpretation

Embed-Net outperformed all the other models throughout each experiment: the highest accuracy achieved and the fastest convergence were secured along with the highest recall. This is due to the fact that categorical embedding layers transform symbolic IoMT features into compact and semantically meaningful vectors. Such embeddings effectively model relationships among categorical attributes, which is hard to achieve with the more traditional encoder mechanisms.

4.2.1 Accuracy and Detection Performance

Embed-Net showed near-perfect accuracy values of about 99.9% on the datasets tested. It also resulted in very high recall and an extremely low false-negative rate, which is especially critical in medical contexts where one intrusion may alter clinical readings or disrupt medical workflows and patient safety. The considerable recall refers to its strong detection across a wide variety of threat scenarios, including rare ones that have low volumes of attacks.

4.2.2 Training Behavior and Convergence Trends

12 As illustrated in Figure 4.1 - Figure 4.2, the training and validation loss curves for Embed-Net converge rapidly to very low values as the number of epochs increases. The gap between training and validation losses remains minimal, indicating strong generalization and limited overfitting.

Which evaluates performance across varying batch sizes, shows that Embed-Net remains stable even with larger batch sizes. Although smaller batch sizes can lead to slightly faster initial learning, Embed-Net maintains consistently high accuracy across all batch configurations.

4.2.3 Computational Considerations

Despite the increased complexity associated with Embed-Net because of the embedding and deep dense layers compared to Deep-SVM-Net, the time required for inference is still satisfactory enough to be deployed in hospital gateway servers or IDS systems that utilize cloud assistance. Through the utilization of dense embeddings rather than one-hot encodings, it greatly alleviates sparsity and saves memory.

4.3 Conv-Net-SVM: Results and Interpretation

The Conv-Net-SVM architecture is an amalgamation of both feature extraction through convolution and classification using an SVM framework, with good results, especially where there exist patterned distributions of IoMT traffic.

4.3.1 Accuracy and Structural Pattern Recognition

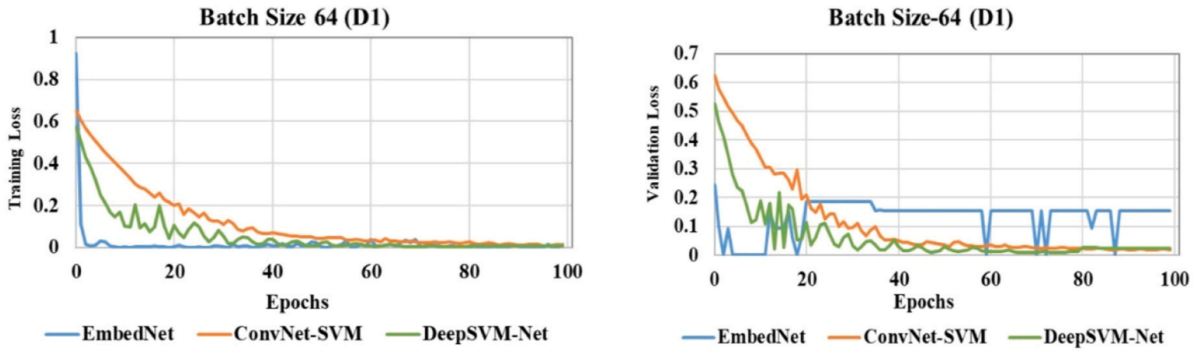
The accuracies of Conv-Net-SVM were in the neighborhood of 99.5% - 99.6%, placing second place out of the three models tested. The Convolutional layers in the Conv-Net-SVM are able to learn patterns that represent structural attack behavior, such as repeat patterns in DDoS attacks, reconnaissance scans, and probes.

4.3.2 Convergence Stability and Epoch Analysis

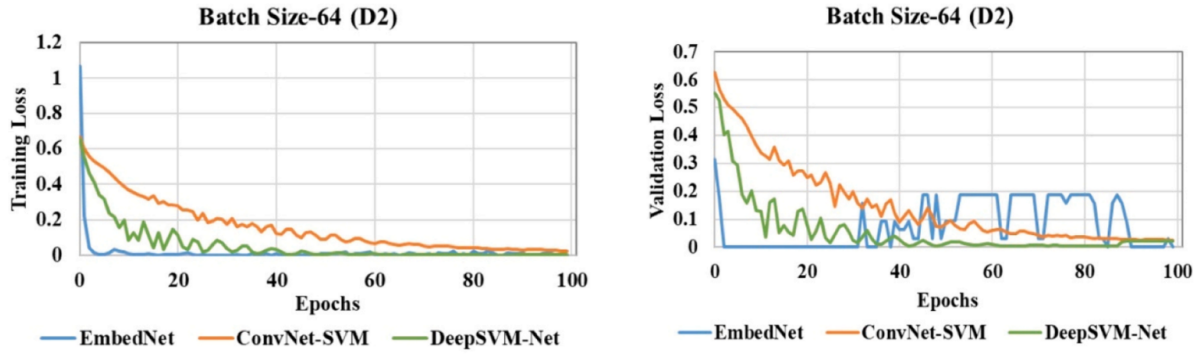
As illustrated in Figures 4.1-4.2, both the training and validation curves of Conv-Net-SVM tend to converge well with increasing number of epochs, although less rapidly compared to Embed-Net. The curves experience some oscillations during early epochs, which are due to their sensitivity to changes in feature transformations and convolutional initialization.

4.3.3 Effect of Batch Sizes

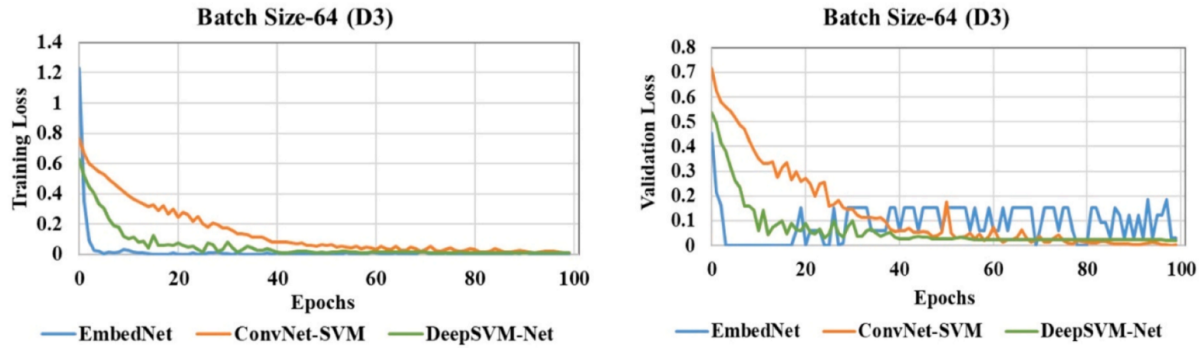
Figures 4.1-4.2 demonstrate that Conv-Net-SVM is generally more sensitive to differences in batch sizes compared to Embed-Net. This means that smaller batch sizes tend to result in somewhat unstable training while larger batch sizes tend to result in smooth convergence.



(a) Training Loss over 100 Epoch on Dataset 1

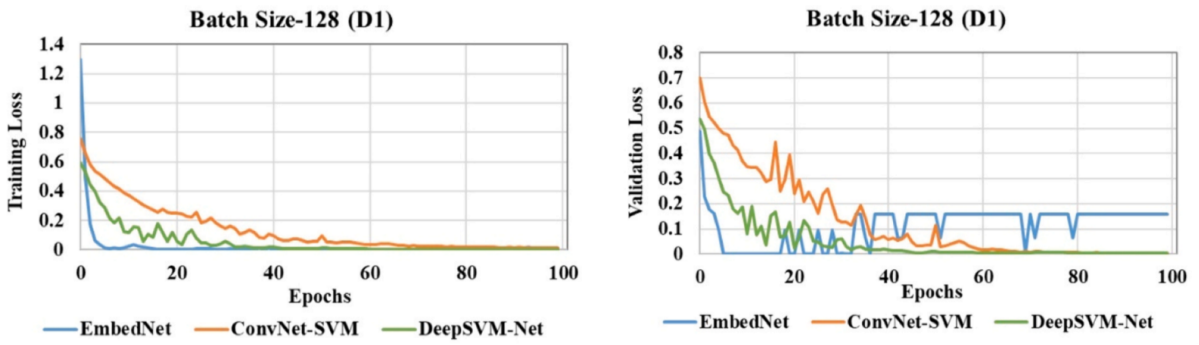


(b) Training Loss over 100 Epoch on Dataset 2

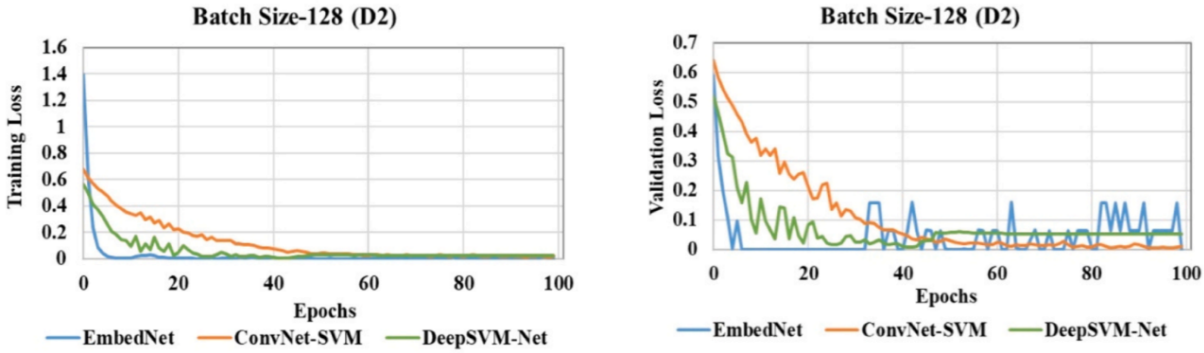


(c) Training Loss over 100 Epoch on Dataset 3

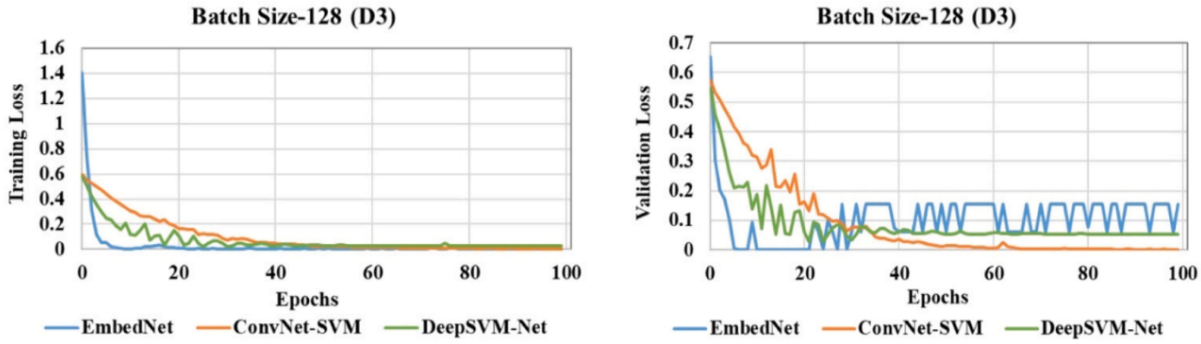
Figure 4.1: Training & validation loss-curves of Embed-Net, Conv-Net-SVM, and Deep-SVM-Net across datasets Data1, Data2, and Data3 over 100 epochs, batch size of 64.



(a) Training Loss over 100 Epoch on Dataset 1

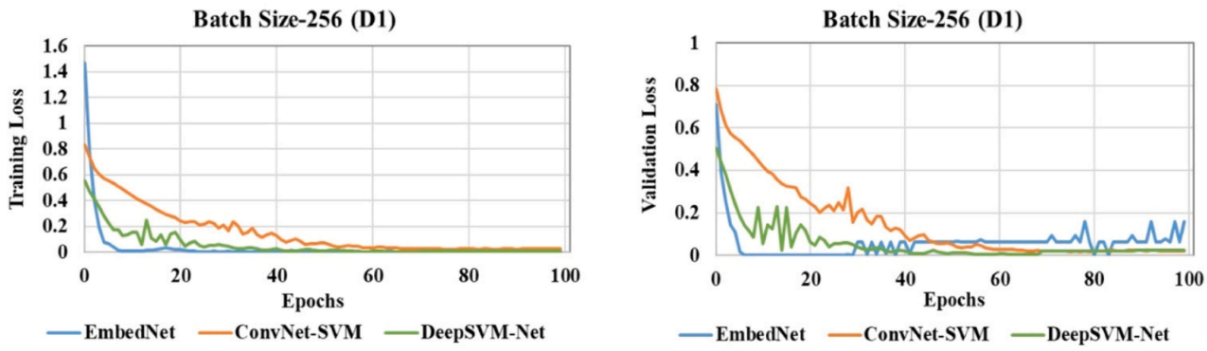


(b) Training Loss over 100 Epoch on Dataset 2

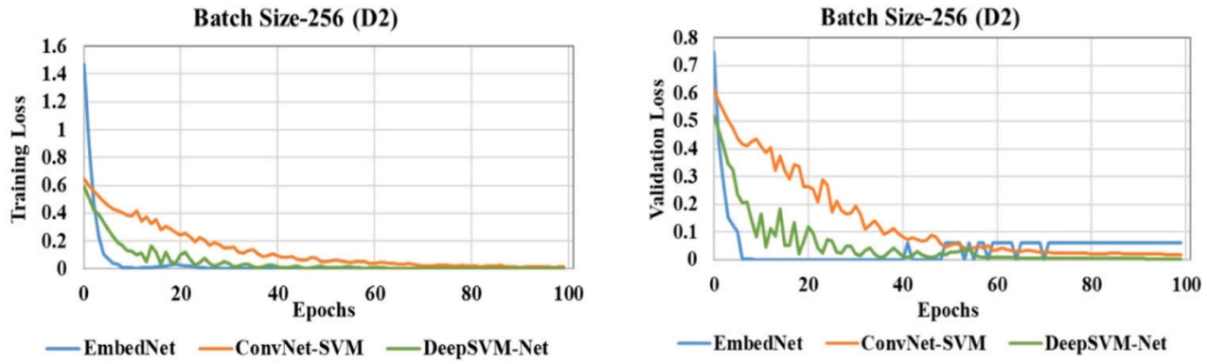


(c) Training Loss over 100 Epoch on Dataset 3

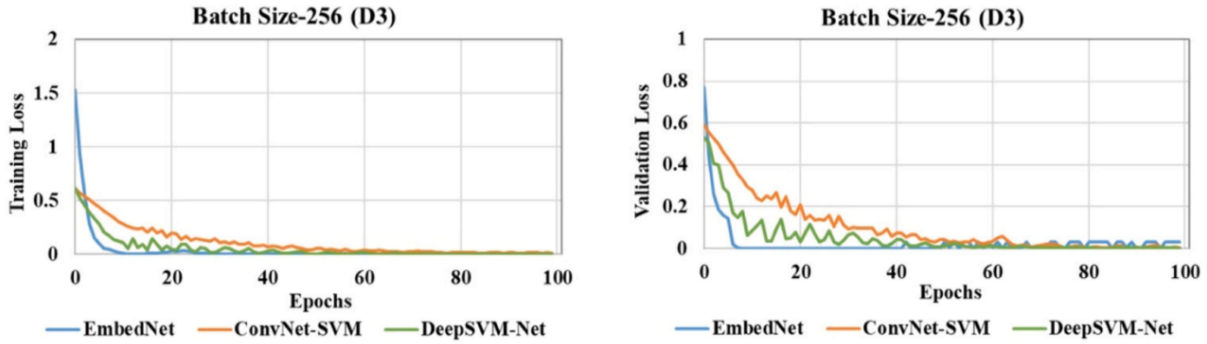
Figure 4.2: Training & validation loss-curves of Embed-Net, Conv-Net-SVM, and Deep-SVM-Net across datasets Data1, Data2, and Data3 over 100 epochs, batch size of 128.



(a) Training Loss over 100 Epoch on Dataset 1



(b) Training Loss over 100 Epoch on Dataset 2



(c) Training Loss over 100 Epoch on Dataset 3

Figure 4.3: Training & validation loss-curves of Embed-Net, Conv-Net-SVM, and Deep-SVM-Net across datasets Data1, Data2, and Data3 over 100 epochs, batch size of 256.

Proposed Models	Training Dataset	Testing Dataset	Accuracy	Precision	Recall	F1-Score
Embed-Net	ECU-IoHT	NF-BoT-IoT	0.9845	0.9820	0.9835	0.9827
	ECU-IoHT	WUSTL-HDRL–2024	0.9788	0.9765	0.9772	0.9768
	NF-BoT-IoT	ECU-IoHT	0.9852	0.9830	0.9845	0.9837
	NF-BoT-IoT	WUSTL-HDRL–2024	0.9772	0.9750	0.9758	0.9754
	WUSTL-HDRL–2024	ECU-IoHT	0.9830	0.9810	0.9820	0.9815
	WUSTL-HDRL–2024	NF-BoT-IoT	0.9755	0.9735	0.9745	0.9740
Conv-Net-SVM	ECU-IoHT	NF-BoT-IoT	0.9795	0.9770	0.9780	0.9775
	ECU-IoHT	WUSTL-HDRL–2024	0.9725	0.9702	0.9730	0.9719
	NF-BoT-IoT	ECU-IoHT	0.9810	0.9790	0.9801	0.9795
	NF-BoT-IoT	WUSTL-HDRL–2024	0.9733	0.9710	0.9720	0.9715
	WUSTL-HDRL–2024	ECU-IoHT	0.9785	0.9760	0.9770	0.9765
	WUSTL-HDRL–2024	NF-BoT-IoT	0.9715	0.9695	0.9701	0.9701
Deep-SVM-Net	ECU-IoHT	NF-BoT-IoT	0.9888	0.9865	0.9875	0.9870
	ECU-IoHT	WUSTL-HDRL–2024	0.9842	0.9820	0.9830	0.9825
	NF-BoT-IoT	ECU-IoHT	0.9875	0.9855	0.9865	0.9860
	NF-BoT-IoT	WUSTL-HDRL–2024	0.9790	0.9790	0.9790	0.9795
	WUSTL-HDRL–2024	ECU-IoHT	0.9860	0.9840	0.9850	0.9845
	WUSTL-HDRL–2024	NF-BoT-IoT	0.9795	0.9775	0.9785	0.9780

Figure 4.4: Table 4.1 : Working architecture of Deep-SVM-Net model.

Discussion on Cross-Dataset Generalization Performance

Table **??** shows the cross-dataset generalization performance of the proposed intrusion detection models—Embed-Net, Conv-Net-SVM, and Deep-SVM-Net—when trained and tested on three IoMT datasets, namely ECU-IoHT, NetFlow(NF)-BoT-IoT, and WUSTL-HDRL–2024. The table provides insight into the robustness, flexibility, and transferability of the described models in several IoMT scenarios. Since IoMT traffic patterns vary significantly across different datasets, a high accuracy score in the cross-dataset testing indicates that the model can learn generalizable feature representations rather than memorizing dataset-specific behavior.

4.3.4 Computational Efficiency

Due to the presence of convolutional layers, Conv-Net-SVM incurs higher computational cost compared to Embed-Net and Deep-SVM-Net. Practical deployment may thus require GPU acceleration or high-capacity fog or edge servers. Nevertheless, its strong ability to

exploit spatial correlations in traffic patterns makes it highly valuable in settings where detecting structurally repetitive or multi-stage attacks is a priority.

Overall, Conv-Net-SVM emerges as a good middle solution since it provides a combination of high accuracy and high-level pattern recognition, although with increased computational complexity.

4.4 Deep-SVM-Net: Results and Interpretation

As the name suggests, Deep-SVM-Net addresses both deep dense representation learning as well as margin-based output layer similar to SVM architecture. It is supposed to be lightweight with high accuracy performance.

4.4.1 Accuracy and Margin Optimization

High accuracy was provided by Deep-SVM-Net, reaching almost 99.8%. The model worked successfully with all datasets. High separability provided by the margin-based output layer contributed to the successful work of the proposed model. Although its accuracy is slightly lower compared to Embed-Net, this tradeoff seems appropriate in terms of real-time implementation on IoT devices.

4.4.2 Training and Validation Behavior

Figures 4.1 to 4.2 illustrate that Deep-SVM-Net has fast convergence rates and demonstrates stability during training. Though the final loss achieved by Deep-SVM-Net is marginally higher than that of Embed-Net, the gap between training and validation losses is not much, indicating better generalization without any chances of overfitting.

4.4.3 Efficiency and Deployment Readiness

Amongst all three methods, Deep-SVM-Net is the most efficient model as it does not employ any convolutional layers but performs only dense and non-linear transformations. Therefore, Deep-SVM-Net is more deployable on:

- The IoMT gateways are with moderate compute capacity.
- Edge devices.

- The wearable and portable medical systems.
- The Embedded controllers are in smart medical equipments.

It is the high speed and also compact architecture compensate for the small drop in accuracy compared to the Embed-Net.

4.5 Comparative Discussion of All Three Models

The combined results are reveal the complementary strengths and also trade-offs among the three architectures.

4.5.1 Overall Accuracy

- **Embed-Net:** Highest accuracy ($\sim 99.9\%$)
- **Deep-SVM-Net:** Very high accuracy ($\sim 99.8\%$)
- **Conv-Net-SVM:** Slightly lower, around 99.5–99.6%

4.5.2 False-Negative Rates

Embed-Net has the least amount of false negative rates compared to the other models, making it the best choice for critical IoMT applications due to the fact that false negatives may have fatal consequences. The other two algorithms, namely Deep-SVM-Net and Conv-Net-SVM, have low FNR values as well.

4.5.3 Computational Efficiency

- **Deep-SVM-Net:** In this fastest and most lightweight in terms of computation and also in terms of memory.
- **Embed-Net:** In this moderate computational requirements as well as feasible for gateway or cloud deployment.
- **Conv-Net-SVM:** In this highest computational cost due to the convolutional operations.

4.5.4 Semantic Categorical Feature Understanding

However, Embed-Net exhibited better results than other approaches for processing IoMT attribute categories because of the embedding layers, which managed to discover semantics in symbols like protocols, service types, and device identifiers.

From the comparative analysis, the following can be concluded:

- The Embed-Net is the preferred choice where maximum accuracy and also the minimal false negatives are required.
- In the Deep-SVM-Net offers an excellent balance between accuracy and also in the efficiency for constrained devices.
- In the Conv-Net-SVM, particularly advantageous in the environments dominated by structured, pattern-rich attack behaviors.

These findings reinforce the value of deep learning (DL) architectures that tailored to IoMT-specific characteristics for the enhancing the effectiveness and the practicality of intrusion detection systems.

Chapter 5

CONCLUSION AND FUTURE SCOPE

The ever-increasing need for IoMT in real-time monitoring of patients, automatic diagnosis, and decision-making processes within healthcare institutions means that cybersecurity is now a crucial component of modern healthcare services. As depicted in Figure 1.1, IoMT systems encompass several layers of connected components like sensors, gateways, cloud computing, and medical software, hence providing multiple opportunities for attack. While the classic IDS systems have been effective within the conventional network environment, they have proven inadequate in addressing the heterogeneous nature of cyber threats in current medical infrastructures. This study will try to identify the weaknesses of such schemes by deploying three different types of deep learning architectures: Embed-Net, Conv-Net-SVM, and Deep-SVM-Net.

5.1 Conclusion

As evident from the analysis, Embed-Net proved to be the best model in terms of balance and superior performance as compared to other two models. The model used the concept of embedding to deal with heterogeneous IoMT features by converting categorical features to vectors. Semantic similarities between device identifier features, protocol flag features, and service patterns were identified using Embed-Net. Feature dimension was also significantly reduced by the model while maintaining key feature relations. Embed-Net also showed the best accuracy, the least false negative rate, and stable convergence for all epochs and batch configurations, as shown in Figures 4.1 through 4.2. It can be clearly concluded from this that Embed-Net has a high potential to identify complex cyber threats within a medical environment.

Deep-SVM-Net model proved to be computationally efficient along with high accuracy. The combination of SVM-like output layer with the densely stacked deep learning layer made the model classify effectively in the case of noisy or overlapping IoMT []. Additionally, the lightweight nature of Deep-SVM-Net makes it the preferred option for use as an intrusion detection system for edge IoMT devices such as wearable and portable devices.

In general, this study finds that there is no universally ideal model for all IoMT applications. Each of the three models studied here performs exceptionally well in its own set of operational conditions.

- **Embed-Net** is the best suited for large-scale hospital networks and also cloud-assisted IDS deployments, where high accuracy and the rich modeling of categorical features are very critical.
- **Conv-Net-SVM** is effective in the environments requiring the strong spatial feature extraction, the particularly for patterned attack behaviors.
- **Deep-SVM-Net** is the well-suited for low-power medical devices that demand the fast inference with the minimal computational overheads.

This the comparative evaluation is therefore shows that the advanced deep learning (DL) models, if carefully crafted to accommodate the peculiar data characteristics of IoMT, can significantly improve the detections capability of IDS without compromising operational practicality.

5.2 Practical Implications of the Proposed IDS Framework

The importance of implementing intelligent IDS for IoMT systems goes far beyond theoretical analysis of system performance. Healthcare facilities in modern days are becoming dependent on various digital systems which help monitor patients, respond to emergencies, conduct medical imaging procedures, conduct diagnostics, and control clinical workflow. Increasing reliance on connected healthcare technology results in higher stakes in the case of cybersecurity failure.

The proposed IDS model using a deep learning architecture has numerous real-life applications in healthcare. For instance, in large hospitals where thousands of devices constantly communicate through different networks, an intelligent IDS can constantly monitor network traffic and detect abnormalities in the communication pattern. Timely detection of malicious behavior will help avoid any potential disruption of services and ensure the confidentiality of patients' personal data.

In particular, Embed-Net, with its ability to effectively deal with heterogeneous categorical features, will be highly effective in the case of a central hospital infrastructure where

there is complex communication among various medical devices. Learning semantic relationship between protocol-level attributes allows to detect even slight alterations in attacks and thus recognize various attacks that cannot be recognized by traditional security methods.

Conv-Net-SVM can be applied with practical benefits in scenarios wherein attacks display significant structural or sequential characteristics. In healthcare facilities, there is usually a lot of periodic traffic generated from monitoring devices, diagnostic systems, or medical sensors. The ability of the convolutional technique to extract useful features helps detect any irregularities such as volumetric attacks, scan attacks, or botnet activity.

The use of Deep-SVM-Net in practical deployment can help overcome the challenge associated with limited computation capability in lightweight medical environments. Portable medical systems, wearable medical monitoring systems, infusion devices, and embedded medical gateway devices have low computing power, and hence require a lightweight system like Deep-SVM-Net that does not involve too much memory usage.

In terms of practical implementation, another aspect that is noteworthy is the effect of cybersecurity attacks on healthcare reliability. In such cases, hospital systems might get disrupted, affecting procedures and delaying emergency treatment. Such intelligent intrusion detection systems can, therefore, provide not just technical support, but also instill confidence in digital health care solutions.

Moreover, the suggested framework is scalable in the context of today's healthcare systems. With the ever-growing number of connected medical devices, it becomes necessary for hospitals to have intrusion detection systems that can scale up to meet rising traffic demands without compromising on performance. The use of a modular system and the preprocessing technique used in the study help in achieving this goal.

In conclusion, the deep learning intrusion detection framework that has been proposed in this study holds immense promise in terms of enhancing security in the future of healthcare systems.

5.3 Limitations of the Present Study

Despite the high detection effectiveness and computational efficiency shown by the suggested intrusion detection framework on several IoMT datasets, there are some limitations present in this study. Pointing out these limitations is crucial since it will guide further

improvements on the model and create realistic expectations in regard to its applications.

A limitation of this study lies in the use of benchmark datasets in the process of modeling and evaluating the performance of the proposed models. Datasets like ECU-IoHT, WUSTL-HDRL-2024, and NF-BoT-IoT have traffic patterns that resemble the real traffic generated in healthcare settings. However, the traffic generated in actual health care infrastructures consists of highly unpredictable communication behavior, unknown traffic load levels, and continuously changing attack strategies.

Another limitation of this study is that no real-life application experiment was conducted to test the viability of real-time implementation of the model. The evaluation of this paper's proposed intrusion detection models is mainly done using offline experimental analysis. Even though important measurements of accuracy and recall were provided, there could be some other factors encountered when implementing the models into real-time settings.

In terms of computational analysis carried out in this research, the emphasis is more on relative efficiency of architecture rather than specific hardware benchmarking. Practical performance will depend on the type of processor, available memory and the type of network infrastructure used in the healthcare settings. Experimentation with embedded devices or edge computing will lead to a better comprehension of practical deployment of the technique.

A notable constraint of the study lies in its inability to address issues associated with adversarial robustness. Recent cyberattacks tend to utilize techniques that adapt and defeat machine-learning detection algorithms. In this case, the research mostly assesses normal intrusion cases but does not look into adversarial cases that aim at deceiving the deep learning model.

Moreover, the deep learning-based intrusion detection approach is mostly interested in differentiating between benign and malicious traffic. However, in practical health care cybersecurity cases, intrusion could involve many classes such as ransomware, denial-of-service attacks, botnet communications, spoofing attacks and reconnaissance activities.

Another important prerequisite of the current research is the availability of training data properly labeled. Nonetheless, the collection of large and properly labeled datasets of traffic generated by healthcare organizations poses significant challenges due to privacy issues and regulations, among others.

Despite these constraints, the proposed model can serve as a sound basis for developing effective IoMT intrusion detection systems. In particular, the study confirms the superiority

of deep learning models tailored to heterogeneous medical traffic in terms of both cybersecurity performance and computational efficiency.

5.4 Future Scope

Even though the experiments conducted on the presented models have provided positive results regarding their performance, there are numerous possibilities for development in the field of cybersecurity for IoMT in the future. They include the following aspects:

1. **Incorporation of Real-Time IoMT Devices**
   The present investigation has relied on benchmark data for its evaluation procedures. For future research, the implementation of such models on real IoMT devices or simulators can be considered, whereby attention will be paid to:

   - Real-time processing latency
   - Energy consumption
   - The communication delay and also throughput

   Therefore such experiments would provided deeper insights into the practical deployments feasibility.

2. **Adaptive and Continual Learning**
   The cyber-threats continually evolves, and the static models may be degrade over the time. Incorporating:

   - Online learning,
   - Continual learning, or
   - The Concept drift adaptation techniques

   These would allow the IDS models to update themselves in the responses to emerging attacks types without complete retraining.

3. **Federated and Privacy-Preserving Learning**
   Given that patient data is the highly sensitive, future generation the IDS systems can be built in conjunction with federated learning models to facilitate collaborative training among various hospitals or clinics without the sharing actual patients info. This will:

- This will improve the robustness of detection by the exposure to the diverse data sources.
- It follows all the privacy regulations and also security policies

4. **Explainable AI for Medical IDS**

   The utilization of explanatory methods like SHAP, LIME, or visualizing attentions may be introduced to allow security specialists and hospital administrators comprehend the reasons why a specific network flow is considered to be malicious. The following points will become extremely important:

   - The building trust in the AI-driven IDS systems
   - Supporting security audits and compliance reporting
   - Assisting in incident response and root-cause analysis

REFERENCES

[1] E. Kabir, J. Hu, H. Wang, G. Zhuo, "A novel statistical technique for intrusion detection systems," *Future Generation Computer Systems*, vol. 79, 2018, pp. 303–318. https://doi.org/10.1016/j.future.2017.01.029.

[2] T. Aldwairi, D. Perera, M. A. Novotny, "An evaluation of the performance of restricted Boltzmann machines as a model for anomaly network intrusion detection," *Computer Networks*, vol. 144, 2018, pp. 111–119. https://doi.org/10.1016/j.comnet.2018.07.025.

[3] S. Aljawarneh, M. Aldwairi, M. B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," *Journal of Computational Science*, vol. 25, 2018, pp. 152–160. https://doi.org/10.1016/j.jocs.2017.03.006.

[4] A. Abusitta, M. Bellaiche, M. Dagenais, T. Halabi, "A deep learning approach for proactive multi-cloud cooperative intrusion detection system," *Future Generation Computer Systems*, vol. 98, 2019, pp. 308–318. https://doi.org/10.1016/j.future.2019.03.043.

[5] J. Gu, L. Wang, H. Wang, S. Wang, "A novel approach to intrusion detection using SVM ensemble with feature augmentation," *Computers & Security*, vol. 86, 2019, pp. 53–62. https://doi.org/10.1016/j.cose.2019.05.022.

[6] C. Kim, J. Park, "Designing online network intrusion detection using deep autoencoder Q-learning," *Computers & Electrical Engineering*, vol. 79, 2019, 106460. https://doi.org/10.1016/j.compeleceng.2019.106460.

[7] Y. Zhou, G. Cheng, S. Jiang, M. Dai, "Building an efficient intrusion detection system based on feature selection and ensemble classifier," *Computer Networks*, vol. 174, 2020, 107247. https://doi.org/10.1016/j.comnet.2020.107247.

[8] X. Li, W. Chen, Q. Zhang, L. Wu, "Building auto-encoder intrusion detection system based on random forest feature selection," *Computers & Security*, vol. 95, 2020, 101851. https://doi.org/10.1016/j.cose.2020.101851.

[9] Y. Zhou, T. A. Mazzuchi, S. Sarkani, "M-adaboost-A based ensemble system for network intrusion detection," *Expert Systems with Applications*, vol. 162, 2020, 113864. https://doi.org/10.1016/j.eswa.2020.113864.

[10] S. P. R. M., P. K., M. P. Maddikunta, S. Koppu, T. R. Gadekallu, C. L. Chowdhary, M. Alazab, "An effective feature engineering for DNN using hybrid PCA-GWO for

intrusion detection in IOMT architecture," *Computer Communications*, vol. 160, 2020, pp. 139–149. https://doi.org/10.1016/j.comcom.2020.05.048.

[11] M. Ahmed, S. Byreddy, A. Nutakki, L. F. Sikos, P. Haskell-Dowland, "ECU-ioht: a dataset for analyzing cyberattacks in Internet of health things," *Ad Hoc Networks*, vol. 122, 2021, 102621. https://doi.org/10.1016/j.adhoc.2021.102621.

[12] S. K. Shahzad, D. Ahmed, M. R. Naqvi, M. T. Mushtaq, M. W. Iqbal, F. Munir, "Ontology driven smart health service integration," *Computer Methods and Programs in Biomedicine*, vol. 207, 2021, 106146. https://doi.org/10.1016/j.cmpb.2021.106146.

[13] M. Alazab, R. A. Khurma, A. Awajan, D. Camacho, "A new intrusion detection system based on Moth–Flame optimizer algorithm," *Expert Systems with Applications*, vol. 210, 2022, 118439. https://doi.org/10.1016/j.eswa.2022.118439.

[14] E.-H. Qazi, M. Imran, N. Haider, M. Shoaib, I. Razzak, "An intelligent and efficient network intrusion detection system using deep learning," *Computers & Electrical Engineering*, vol. 99, 2022, 107764. https://doi.org/10.1016/j.compeleceng.2022.107764.

[15] S. Patil, V. Varadarajan, S. M. Mazhar, A. Sahibzada, N. Ahmed, O. Sinha, S. Kumar, K. Shaw, K. Kotecha, "Explainable artificial intelligence for intrusion detection system," *Electronics*, vol. 11, no. 19, 2022, 3079. https://doi.org/10.3390/electronics11193079.

[16] I. F. Kilincer, F. Ertam, A. Sengur, R.-S. Tan, U. Rajendra Acharya, "Automated detection of cybersecurity attacks in healthcare systems with recursive feature elimination and multilayer perceptron optimization," *Biocybernetics and Biomedical Engineering*, vol. 43, no. 1, 2023, pp. 30–41. https://doi.org/10.1016/j.bbe.2022.11.005.

[17] F. Mosaiyebzadeh, S. Pouriyeh, R. M. Parizi, M. Han, D. M. Batista, "Intrusion detection system for IOHT devices using federated learning," in *IEEE INFOCOM 2023 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2023. https://doi.org/10.1109/infocomwkshps57453.2023.10225932.

[18] T. Thulasi, K. Sivamohan, "LSO-CSL: light spectrum optimizer-based convolutional stacked long short term memory for attack detection in IOT-based healthcare applications," *Expert Systems with Applications*, vol. 232, 2023, 120772. https://doi.org/10.1016/j.eswa.2023.120772.

[19] J. Azimjonov, T. Kim, "Designing accurate lightweight intrusion detection systems for IOT networks using fine-tuned linear SVM and feature selectors," *Computers &*

Security, vol. 137, 2024, 103598. https://doi.org/10.1016/j.cose.2023.103598.

[20] Y. Zhang, D. Zhu, M. Wang, J. Li, J. Zhang, "A comparative study of cyber security intrusion detection in healthcare systems," *International Journal of Critical Infrastructure Protection*, vol. 44, 2024, 100658. https://doi.org/10.1016/j.ijcip.2023.100658.

[21] A. Nazir, J. He, N. Zhu, S. S. Qureshi, S. U. Qureshi, F. Ullah, A. Wajahat, M. S. Pathan, "A deep learning-based novel hybrid CNN-LSTM architecture for efficient detection of threats in the IOT ecosystem," *Ain Shams Engineering Journal*, vol. 15, no. 7, 2024, 102777. https://doi.org/10.1016/j.asej.2024.102777.

[22] A. D. Aguru, S. B. Erukala, "A lightweight multi-vector DDoS detection framework for IOT-enabled mobile health informatics systems using deep learning," *Information Sciences*, vol. 662, 2024, 120209. https://doi.org/10.1016/j.ins.2024.120209.

[23] R. Kumar, A. Aljuhani, D. Javeed, P. Kumar, S. Islam, A. K. M. N. Islam, "Digital Twins-Enabled zero touch network: a smart contract and explainable AI integrated cybersecurity framework," *Future Generation Computer Systems*, vol. 156, 2024, pp. 191–205. https://doi.org/10.1016/j.future.2024.02.015.

[24] Y. K. Saheed, O. H. Abdulganiyu, T. A. Tchakoucht, "Modified genetic algorithm and fine-tuned long short-term memory network for intrusion detection in the Internet of things networks with edge capabilities," *Applied Soft Computing*, vol. 155, 2024, 111434. https://doi.org/10.1016/j.asoc.2024.111434.

[25] S. S. Chintapalli, S. P. Singh, J. Frnda, P. Bidare Divakarachari, V. L. Sarraju, P. Falkowski-Gilski, "OOA-modified Bi-LSTM network: an effective intrusion detection framework for IOT systems," *Heliyon*, vol. 10, no. 8, 2024, e29410. https://doi.org/10.1016/j.heliyon.2024.e29410.

[26] G. Lazrek, K. Chetioui, Y. Balboul, S. Mazer, M. El Bekkali, "An RFE/ridge-ML/DL based anomaly intrusion detection approach for securing IOMT system," *Results in Engineering*, vol. 23, 2024, 102659. https://doi.org/10.1016/j.rineng.2024.102659.

[27] I. Ioannou, P. Nagaradjane, P. Angin, P. Balasubramanian, K. J. Kavitha, P. Murugan, V. Vassiliou, "Gemlids-Miot: a Green effective machine learning intrusion detection system based on federated learning for medical IOT network security hardening," *Computer Communications*, vol. 218, 2024, pp. 209–239. https://doi.org/10.1016/j.comcom.2024.02.023.

[28] N. Sharma and P. G. Shambharkar, "Transforming security in internet of medical things with advanced deep learning-based intrusion detection frameworks," Applied

Soft Computing, vol. 180, 113420, 2025. doi: 10.1016/j.asoc.2025.113420.

Shailender Kumar

AshishKumar_thesisreport

paper

Document Details

Submission ID

trn:oid:::27535:140626387

Submission Date

May 27, 2026, 12:40 PM GMT+5:30

Download Date

May 27, 2026, 12:42 PM GMT+5:30

File Name

AshishKumar_thesisreport.pdf

File Size

2.0 MB

48 Pages

11,980 Words

71,874 Characters

14% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

- **97** Not Cited or Quoted 10%
  Matches with neither in-text citation nor quotation marks
- **11** Missing Quotations 1%
  Matches that are still very similar to source material
- **14** Missing Citation 3%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

11% Internet sources
12% Publications
12% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.