ISSN: 2093-5374 / E-ISSN: 2093-5382

Advancing IoMT Security: Machine Learning-Based Detection and Classification of Multi-Protocol Cyberattacks

Loiy Alsbatin[1*], Basem Mohamad Alrifai[2], Firas Zawaideh[3], and Tareq A. Alawneh[4]

[1*] Electrical Engineering Department, Al-Balqa Applied University, Amman, Jordan.
loiy.alsbatin@bau.edu.jo, https://orcid.org/0000-0002-3892-698X

[2]Faculty of Information Technology, Computer Science Department, Jadara University, Irbid, Jordan. b.rifai@jadara.edu.jo, https://orcid.org/0000-0002-4510-1011

[3]Faculty of Information Technology, Networks and Cybersecurity Department, Jadara University, Irbid, Jordan. f.zawaideh@jadara.edu.jo, https://orcid.org/0000-0001-6063-1179

[4]Electrical Engineering Department, Al-Balqa Applied University, Amman, Jordan.
tareq.alawneh@bau.edu.jo, https://orcid.org/0000-0002-2400-1599

Received: March 01, 2025; Revised: April 08, 2025; Accepted: May 12, 2025; Published: June 30, 2025

Abstract

The increasing vulnerabilities in the Internet of Medical Things (IoMT) necessitate advanced cyberattack detection and classification mechanisms, particularly multi-protocol attacks that compromise device functionality and patient safety. The study addresses the lacuna in detecting multi-protocol cyberattacks in IoMT networks by developing a new dataset and applying machine learning algorithms to improve detection efficiency. The study employs a robust research design with simulated network traffic to train Random Forests (RF), Support Vector Machines (SVM), and Artificial Neural Networks (ANN). The dataset spans a diverse range of attack scenarios to permit extensive feature engineering and performance measurements with precision, recall, and F1 scores. The results indicate that the RF model is more accurate in detecting complex attacks like U2R with a score of 0.74. Despite challenges in differentiating some attack categories, the study highlights the SVM model's potential for handling ambiguous cases. This work contributes a foundational dataset and taxonomy for future research, allowing for enhanced security testing of IoMT devices. It emphasizes the need for interdisciplinary collaboration to develop scalable, resource-efficient, and context-aware solutions. Practical implications include real-time intrusion detection for hospital networks, while limitations, such as reliance on synthetic data, underscore the need for broader dataset diversity. The findings underscore the critical importance of proactive measures to mitigate evolving threats, safeguard IoMT environments, and ensure the privacy and security of sensitive medical data. This research sets the stage for future advancements in IoMT security, integrating adaptive machine-learning techniques to address emerging cyber threats effectively.

Keywords: IoMT Security, Multi-Protocol Cyberattacks, Machine Learning, Intrusion Detection, Healthcare Cybersecurity, Dataset Development.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 16, number: 2 (June), pp. 228-247. DOI: *10.58346/JOWUA.2025.I2.015*

*Corresponding author: Electrical Engineering Department, Al-Balqa Applied University, Amman, Jordan.

1 Introduction

This paper delves into the vulnerabilities of Internet of Medical Things (IoMT) environments and a robust solution to fortify them through security systems and techniques meticulously designed for medical devices and health records (Afifi, 2020). We also introduce an experimental framework to rigorously test and evaluate our security mechanisms. Importantly, we conclude with a promising outlook on the potential transformative effects that our findings and techniques can have on Internet of Things (IoT) security, paving the way for a more secure future for IoT.

Secure IoT environments ensure the safety and privacy of their users. Security mechanisms for IoT can also be helpful for the security of medical environments comprising Medical IoT (MIoT) devices and IoMT platforms (Tariq et al., 2020). Nevertheless, implementing security mechanisms and keeping them up-to-date is a difficult task and can be disrupted by minimal downtime or loss of network connectivity. Furthermore, attacks on an MIoT environment can be more devastating than a regular IoT environment as they can result in patients' lives being endangered, and fewer risks can have more severe consequences for patients than the risk of compromised medical devices and health records. Unfortunately, security is not the primary concern of MIoT vendors, and hospitals are still debating whether to embrace newer technology, given its potential benefits. Progress in this area can potentially change the stance in consideration of medical environments, i.e., safer medical devices and more efficient health monitoring, and it can provide a foundation for security-oriented machine learning research in the IoT (Kamal et al., 2023). In recent years, there has been an increase in security research for IoT devices and networks, namely anomaly detection and behavior analysis (Madhan & Shanmugapriya 2024). However, very few systems take IoT security from a highly technical level, and studies involve the analysis of specific attacks on IoT protocols to provide a more efficient and organized means of safeguarding IoT devices and networks (Obaidat et al., 2020).

IoMT devices, such as insulin pumps, Holter monitors, and wearable fitness trackers, are an innovative medical device class becoming increasingly prevalent in patient care. The Food and Drug Administration (FDA) defines IoMT as medical devices that connect to smartphones and other devices using wireless or wire connections. IoMT devices serve to enhance patient involvement in their care. IoMT devices tend to provide healthcare professionals with a complete picture of a patient's health through continuous monitoring that allows real-time information (Adeniyi et al., 2021). IoMT devices have revolutionized healthcare delivery. The new devices can monitor long-term condition patients to enable timely interventions to be provided if required. Through IoMT devices, patients can be at home without hospital visits that can lead to more complications and eventually save their lives. Furthermore, using IoMT devices enhances patient care quality through convenience and efficiency. In today's era of technology, IoMT devices signify advancement and represent a good investment in healthcare. Such medical devices such as insulin pumps, Holter monitors, and wearable exercise tracking devices have gained popularity due to their efficiency in patient care. FDA-approved IoMT devices describe medical devices that integrate with smartphones and other devices using wireless or wire connections. The integration allows patients to actively participate in their healthcare (Dwivedi et al., 2022). The main advantage of IoMT devices is that they provide healthcare professionals with a complete picture of a patient's health. The devices provide real-time information through continuous monitoring that allows medical professionals to make informed decisions and provide customized treatment (Manickam et al., 2022). The continuous stream of information through IoMT devices ensures that patient health changes are detected early and attended to (Choudhary & Verma 2025).

For example, IoMT devices can monitor those with long-term conditions and help inform providers that a patient needs intervention. IoMT device remote monitoring can help prevent more severe health complications and keeps patients out of hospitals while preserving their health and their lives (Manickam et al., 2022). The quality of patient care is enhanced and more convenient through IoMT device use. In the digital transformation era of healthcare, IoMT devices offer a way forward and a clear investment in healthcare.

Ultimately, IoMT devices unlock patient-centric healthcare. By giving control to individuals to monitor and manage their health, such devices create a proactive healthcare culture (Malhotra & Joshi 2025). As IoMT devices become part of healthcare, the sector advances to a more integrated and effective healthcare future with improved patient outcomes and medical technology innovations (Ashfaq et al., 2022).

Utilizing several layers of protocols in the Open Systems Interconnection (OSI) model, some of the attacks such as man-in-the-middle (MiM) can be orchestrated to intercept sensitive information. In most cases, intercepted information is utilized as a stepping point to attack using several vectors through several protocols with the aim to attack system vulnerabilities (Pavlidis, 2020). The aim of such attacks is to disrupt network systems and attached devices by traversing several layers of protocols with the aim to identify potential vulnerabilities that can be utilized to attack in the future.

Handling complex multi-vector and multi-protocol attacks is a serious challenge in efficiently detecting them as cyberattacks (Ahmed et al., 2022). The challenge is largely due to the fact that more and more interconnected devices have different protocols used by them, making it difficult to identify a harmful event as a cyberattack. Mislabeling such events as cyberattacks results in a high rate of false positives in detection systems that can lead to unnecessary mitigation measures and divert attention and resources to actual threats. Apart from this, other limiting factors have to be considered in IoMT systems. Such systems include computationally constrained devices and operate on constrained bandwidth network connections (Shen et al., 2024). As such, applying current detection methods to an IoT device becomes very inconvenient since they require resources (Dixit & Bhagat 2021). In other cases, applying such techniques involves offloading data to a cloud server or a similar network gateway to have it evaluated. The mechanism involves sending the data to a remote point to be evaluated, examined to check if it has some behavioral patterns that match those of a familiar cyberattack. Unfortunately, such a mechanism's high computation and offloading requirements of data make offsite evaluation practically infeasible and prohibitively expensive as a solution (Anagnostopoulos et al., 2022).

Our research aims to improve machine learning-based detection and classification of cyberattacks on IoMT devices by focusing on multi-protocol attacks. The first objective is to build and foster a research community interested in securing IoMT devices by turning the latest advances in AI/ML techniques into safe and effective healthcare delivery. To accomplish this, we plan to leverage a small portion of National Institutes of Health (NIH) research administrative supplements to organize a community-wide interdisciplinary workshop that brings together researchers in machine learning, security, medical device development, and medical practitioners. The second objective is to develop a critical mass of researchers interested in IoMT security at the host institution by training new researchers. The justification for this objective is that no researchers at UIC are pursuing a study at the intersection of medical devices and security. This will be achieved by training a PhD student in machine learning and security of medical devices. Assessment of the training and the student's potential to conduct future research in this area will come from the quality of coursework, successful participation in the broader research community, and publication and presentation of research results at the host institution and external research venues. The third and final objective is to produce technology and knowledge transfer to improve the security of current and future generations of medical devices. This will be accomplished by engaging in an ongoing dialogue with industry and governmental stakeholders on IoMT security and providing them with evidence-based knowledge of vulnerabilities and efficient methods for attacks on medical devices and the data they collect and transmit. This dialogue will fulfill the dedication to improving the security and preserving the privacy of medical devices and the data they handle.

This research makes the following contributions to the field of IoMT security. First, we are the first to construct a multi-protocol cyber-attack dataset for the IoMT, which uncovers the potential threat of the multi-protocol cyber-attacks on the IoMT and also promotes future related research on cyber-attack detection and classification on the IoMT. One way to better understand and mitigate security risks to the IoMT, researchers and practitioners could create custom attack IDS/IPS solutions. Better understanding and mitigation start with good data and diverse multi-protocol cyber-attack data for the IoMT, which is the first step in that direction. We have found and categorized more than 18 attack scenarios defined by our taxonomy, meaning attackers have quite a list of potential targets on the IoMT. This dataset and taxonomy created from it help further understand and mitigate security risks to the IoMT. By looking at the results of this research, system administrators, security professionals, or developers can use our dataset to safely test IoMT devices and networks to determine if they are providing basic security and to help them better understand the current and potential threats. Additionally, other researchers can easily use our dataset and extend it with their data to continue dealing with cyber-attacks from various research angles.

2 Literature Review

2.1 IoMT Security Concerns

The Carbanak gang, a notorious cybercriminal organization, has successfully executed highly sophisticated attacks on banks, resulting in the theft of an astonishing one billion euros. Their modus operandi involves initiating phishing campaigns to gain unauthorized access to victims' computers. Once inside, they navigate through networks, steadily progressing toward systems responsible for handling SWIFT transfers, a financial messaging service (Wang & Hsieh, 2021). This exemplifies a common trend among attackers, as they meticulously follow the trail of valuable data, targeting systems that were not their primary objective initially. Remarkably, even SWIFT, a widely recognized and trusted platform, has been found to possess vulnerabilities that these malicious individuals can exploit (Patmanathan et al., 2023). Furthermore, it is disturbing that attackers have extended their reach to medical fields, specifically targeting patient data. More instances of ransomware attacks on hospital networks have been reported with a concerning frequency of medical records being attacked (Wang & Hsieh, 2021). Such incidents have been thoroughly documented by Brian Krebs, a well-known independent security researcher, in a series of blogs and articles. For a comprehensive understanding of potential threats in the IoMT (Internet of Medical Things) ecosystem, it is essential to study documented vulnerabilities and attack methods specific to IoMT devices. As with other networked platforms such as IoT (Internet of Things) and ICS (Industrial Control Systems), IoMT devices share similar vulnerabilities due to their legacy design such as weak authentication mechanisms, unencrypted communication, and absence of integrity checking (Wang & Hsieh, 2021). These expose the device and patient health information to exploitation. We performed a comprehensive search that resulted in several articles, conference papers, blogs, and other resources that describe vulnerabilities and outline attacks that were not restricted to IoMT but were applicable to IoMT devices as well (Saxena & Mayank, 2021). Such information is essential to formulate strategies to secure IoMT environments.

Lastly, it is notable to mention the FDA MAUDE (Manufacturer and User Facility Device Experience) database, a useful repository of medical device-related adverse events. Notably, there is a documented case in which a patient undergoing an infusion facilitated by an ambulatory medication pump inadvertently discharged a static electric charge by touching an object (Saxena & Mayank, 2021). This sudden discharge temporarily halted the pump's operation, eventually triggering an alarm due to a memory error and motor stall. Consequently, the pump necessitated replacement to ensure the patient's continued care and safety. By considering these various aspects, stakeholders within the IoMT landscape can gain insights into existing vulnerabilities, prevalent attacks, and real-world instances, empowering them to proactively enhance the security and resilience of IoMT devices and systems (Saxena & Mayank, 2021).

2.2 Machine Learning in Cybersecurity

Threats to IoMT devices are increasing, and they are burdened with excessive use and reliance on technology-mediated communications between clinical systems (Sarker, 2021). However, several recent studies show that machine learning algorithms are pretty successful for classifying network traffic; many are used on routine type datasets, including NSL-KDD, KDD99, and some simulated datasets for possible specific IoMT communication (Manickam et al., 2022; Kamal et al., 2023). Some data shows nearly 100% detection of certain types of cyberattacks using SVMs and Neural Network Algorithms (Zhang et al., 2021). In particular, the 100% detection rates are very promising for detecting outgoing attacks that attempt to penetrate external systems (heritage clinical systems), a known problem of IoMT devices in trying to communicate with other clinical systems. Some machine learning algorithms successfully classify cyberattacks, but recent IoMT protocols suggest that multi-protocol attacks may be the most effective strategy for compromising an IoMT system. Unfortunately, IoMT devices are not conducive to soft real-time intrusion detection using machine learning; a common exception is a recent generation of IoMT devices designed for interfacing electronic health record systems, which are relatively similar to non-IoMT clinical systems (Shaukat et al., 2020; Malhotra & Mehra 2021). Finally, while there are many successful algorithms for binary classification of normal and attack behaviors and specific types of attacks, it is unclear whether these algorithms can adapt to the rapid transformation of cyberattacks and evolving communication practices in IoMT devices (Bakhronova 2025). Overall, the success of machine learning algorithms for intrusion detection and classification of cyberattacks makes them a promising approach for future security strategies of IoMT devices (Dixit et al., 2021).

2.3 Gaps in Current Research

There has been a significant increase in recent years in developing machine learning-based Intrusion Detection Systems (IDS) that can detect and prevent attacks on IoT networks. Such systems have largely focused on detecting single-protocol attacks while leaving multi-protocol attacks behind (Saheed et al., 2022). For instance, a system proposed by (Serinelli et al., 2020) demonstrates its efficiency in detecting and preventing CoAP protocol-based Distributed Denial of Service (DDoS) attacks. The system relies on developing a normal device behavior model with public datasets and verifying deviations in this baseline. The strength of such a system is that it has high attack detection efficiency with low false positive rate (Awajan, 2023). Following this concept, we have every reason to believe that a model-based system can significantly enhance detection of multi-protocol attacks if normal behavior model comprises heterogeneous types of network traffic spanning a large number of protocols (Islam et al., 2021). For this purpose, we aim to develop such a model using the strength of a Recurrent Neural Network (RNN). RNNs have been designed to learn sequences and patterns in sequential data and thus can be extremely effective in analyzing IoMT network traffic that can be perceived as a sequence of message exchanges (Kumar et al., 2022). In such a case, RNNs can be equipped with Long Short-Term Memory (LSTM) cells that can preserve information over a long time and update it as new relevant information arrives. Such a feature enables LSTM-based RNNs to be extremely effective in detecting attacks that can be over several messages being exchanged over several protocols over a long time (Saheed et al., 2022). An instance of a multi-protocol attack is a command and control attack, in which the attacker gains control over a single or several devices and utilizes a variety of protocols supported by such devices over a prolonged period to reach their evil intent – such as stealing patient information. Understanding the seriousness of such attacks in near future, we point to the need to have such intrusion detection systems that can efficiently identify, categorize, and counter such attack scenarios. There is a severe lack of such systems (Islam et al., 2021).

Elaborating on this issue, industry players and researchers must come together to address issues of multi-protocol attacks. Continuing to develop and enhance model-based approaches, especially with RNNs using LSTM cells, will assist in strengthening the security position of IoT networks and safeguard critical systems against potential threats (Saheed et al., 2022). It is essential that academia, industry players, and regulatory bodies come together to provide timely detection and prevention against multi-protocol attacks to safeguard sensitive information being transmitted through IoT networks and preserve their privacy and integrity. We can collectively design a more secure and resilient IoT ecosystem (Rahman et al., 2020).

3 Methodology

3.1 Data Collection

The study uses the CIC IoMT Dataset 2024 that was crafted by the (Canadian Institute for Cybersecurity, 2024) at New Brunswick University. The dataset is crafted to simulate real-world IoMT network traffic and consists of both attack traffic and benign traffic. It provides a full suite of packet capture (.pcap) files, network flows, and extracted features that make detection and categorization of cyberattacks in IoMT environments possible. Unlike other conventional datasets such as KDDCup99 or NSL-KDD, the CIC IoMT Dataset 2024 records cyberattacks that cross several protocols and is thus particularly relevant to today's IoMT security research. The dataset records a variety of attack scenarios ranging from DDoS, Man-in-the-Middle (MiTM), ransomware, traffic caused by a botnet, network scanning, and exfiltration attacks. The attacks take place in a laboratory environment with IoMT devices such as medical sensors, patient monitoring systems, and wearable health devices subjected to adversarial traffic. The network traffic is collected using industry-standard packet analyzers and log aggregation software to ensure that information is accurate, formatted, and labeled to be used with machine learning-based intrusion detection systems.

The dataset is presented in a number of formats such as raw packet capture files (.pcap), extracted network flow records in CSV format, and attack-labeled logs. It is a feature-rich dataset with information at a number of layers of the OSI model such as at the TCP/IP and UDP layers and application-layer protocols like MQTT and CoAP that commonly occur in IoMT environments. The dataset size varies with traffic logged in each scenario but is designed with high variability in attack behaviors to make it effective in training and testing machine learning algorithms. The CIC IoMT Dataset 2024 is at the forefront of this research by being utilized as the main training and testing platform for machine learning algorithms. The pre-processing of information is achieved through feature selection, normalization, and encoding methods to feed it to classifiers such as Random Forest (RF), Support Vector Machines (SVM), and Artificial Neural Networks (ANN). The attack-labeled information supports a supervised learning paradigm to permit accurate evaluation of every model's capability to identify and label cyber threats. The availability of traces with more than a single protocol included increases this dataset's value in developing effective security solutions to real-world IoMT environments. The utilization of the CIC IoMT Dataset 2024 in this research assures realism and reproducibility in testing cybersecurity frameworks in medical IoT environments. The extensive documentation and organization of the dataset allow consistent benchmarking of various machine learning algorithms to contribute to advances in IoMT security research and real-world cybersecurity applications in healthcare networks.

3.2 Feature Engineering

In this research step, we need to prepare data to achieve features for machine learning analysis. The data used in this research is the KDDCup99 dataset. After exploring the data, we found that the data types are numerical, definite, and string. The first step in feature engineering is handling missing values. We found that the KDDCup99 dataset has no missing values so that we can continue to the next step (Ngueajio et al., 2022). In some machine learning algorithms, handling missing values is one of the most crucial parts of the prediction phase. If we don't handle the missing values, it will lead to false prediction results (Silva et al., 2020). There are several methods to handle the missing values, such as mean imputation, regression imputation, and prediction modeling using machine learning algorithms. However, as long as our data contains no missing values, we do not need to impute the missing values. The second step is handling the categorical data (Serinelli et al., 2020). Categorical data can take on one of a limited and usually fixed number of possible values (i.e., blood type, eye color, race, gender, etc.). Because most machine learning models only accept numeric values as input, to use this type of data to represent the features in a predictive model, we need to convert it to numerical data (Kumar et al., 2022). Several methods to convert the categorical data include label encoding, one-hot encoding, and binary encoding. In this research, we prefer to use label encoding. Label encoding is a popular encoding technique for handling categorical variables. In this technique, each label is assigned a unique integer based on alphabetical ordering (Ngueajio et al., 2022).

3.3 Model Development

The machine learning models developed in this work encompass a wide range of attack detection and classification algorithms. Decision Tree Aided - Reinforcement Learning (DTARL) was used for its ability to classify decision trees (Islam et al., 2021). DTARL comprises attack detection and classification phases; both phases train and build a decision tree. Bayesian analysis was used due to the probability of change of conditions and the likelihood of the data. The algorithm uses probabilistic graphical models, which are extremely useful when analyzing data. Clustering was used for anomaly-based IDS; two clustering methods were used, both the K-means (Ladoja & Afape, 2024) and Fuzzy C-means (Maharani & Prasetiyowati, 2023). The two compare the differences between the complex and soft clusters.

The ANN is one of the most well-known attack detection and classification algorithm machine learning algorithms. The Multi-Layer Perceptron (MLP) is a prevalent form of an artificial neural network. It has inputs and an output layer with one or more hidden layers; each layer is interconnected via weights and can represent a non-linear decision surface. The inputs are processed in the hidden layers by a set activation function and relevant weights for each layer of nodes; backpropagation was also used to classify attack data encapsulation with techniques such as Deep Packet Inspection (DPI), which will be expanded in section 3.4. Support Vector Machine (SVM) was used alongside a statistical and geometric approach to classify data using an N-dimensional hyperplane (Abdaljawad et al., 2023). This was important for the detection of complicated cyber-attacks in versatile environments. During SVM processing, a kernel function is used to map inputs from the lower dimension into a higher dimension; this makes it possible for the data to be separated when a simple hyperplane does not exist.

3.4 Evaluation Metrics

We proposed a versatile evaluation framework to assess the detection capability of our classifiers, using five-fold cross-validation to reduce evaluation bias. The metrics chosen are appropriate for multi-class problems and take into account true positive (TP), true negative (TN), false positive (FP), and false negative (FN) results. Accuracy is a simple and often misused evaluation measure. It measures the rate of correct classifications by the classifier, but this measure may be misleading in problems with disparate class distributions. Precision measures the relevancy of the results or the measure of exactness. It is the ratio of correctly predicted positive observations to the total predicted positive observations (TP/TP+FP) (Abdaljawad et al., 2023). Low numbers of FP will yield high precision. Recall measures the completeness of the results. It is the ratio of correctly predicted positive observations to all observations in the actual class (TP/TP+FN). High numbers of FN will yield low recall. Both precision and recall will result in a value between 0 and 1, and the harmonic mean of these two values is the F1-score. The F1-score balances both of these measures: a high F1-score means high precision and recall and an F1-score close to zero means low precision and recall (Montoto et al., 2022). Any classifier with a high F1 score is fine but if a decision has to be taken between the two, precision and recall values can be compared individually to determine which is more critical to the application. In addition to all of these measures of evaluation, it is also critical to take into account other factors such as efficiency in terms of computation, scalability, and interpretability. Comparison of the classifiers on these factors can provide a comprehensive picture of their overall performance (Ladoja & Afape, 2024). In addition to this, feature selection algorithms can be utilized to identify the most critical features to classify with and this can improve the performance of the classifiers even more. Another factor to take into account is that of robustness of the classifiers to input noise and outliers. Robust classifiers can handle variability and anomalies in input and this is critical in real-world applications where input will not necessarily be well-behaved and clean. In addition to this, ensemble methods such as bagging, boosting, and stacking can improve classification accuracy (Maharani & Prasetiyowati, 2023). These methods combine multiple classifiers to make more accurate predictions by exploiting the strength of single-classifiers. In general, the evaluation framework presented within this study provides a comprehensive way to evaluate the detection capability of classifiers and can be applied to a range of machine learning issues. Its scalability, adaptability, and robustness make it good to do research and real-world applications (Abdaljawad et al., 2023).

3.5 Methodology Flowchart

For presenting research methodology in clear and concise manner, a flowchart has been developed to depict key steps involved in identifying and classifying multiple-protocol cyberattacks in IoMT settings as shown in Figure 1. The flowchart illustrates step-by-step procedure followed in this research beginning with collection of datasets and proceeding through pre-processing of data to machine learning model development and their performance evaluation. By depicting such steps, research understanding is facilitated and reproducibility is achieved through flowchart of methodology.

The study begins with gathering the CIC IoMT Dataset 2024 as study basis. The dataset is comprised of real-world IoMT network traffic with both benign traffic and attack traffic, collected in a laboratory-controlled environment. The data is collected using packet capture (.pcap) files, network flow logs, and attack-labeled information covering a wide range of cyber threats including DDoS, botnet traffic, ransomware, MiTM attacks, scanning, and exfiltration. Having such a wide variety of attack types assures a realistic dataset that actually replicates real-world IoMT security challenges. The gathered dataset is then preprocessed and feature engineered to make it machine learning-ready. The feature extraction step includes extracting pertinent network features such as protocol-layer statistics, packet sizes, and flow features. Then feature scaling and normalization is done to have consistent data representation, followed by categorical encoding of attack labels to facilitate machine learning model training. Missing values, if any, are also taken care of to prevent biases in model predictions.

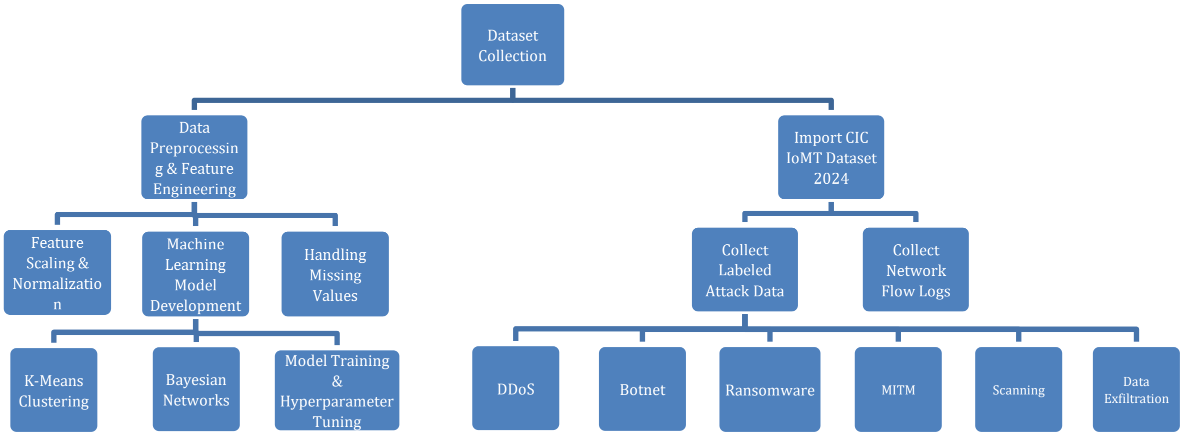
Dataset Collection
Data Preprocessin g & Feature Engineering
Import CIC IoMT Dataset 2024
Feature Scaling & Normalizatio n
Machine Learning Model Development
Handling Missing Values
Collect Labeled Attack Data
Collect Network Flow Logs
K-Means Clustering
Bayesian Networks
Model Training & Hyperparameter Tuning
DDoS
Botnet
Ransomware
MITM
Scanning
Data Exfiltration

Figure 1: Research Methodology Workflow

After pre-processing of data, research continues with machine learning model development to identify cyberattacks and their classifications. Several machine learning algorithms are used to boost detection rates with each offering different advantages. Random Forest (RF) is used due to providing high detection accuracy to identify complex attack patterns, while Support Vector Machine (SVM) is used due to handling uncertain cases. ANN are used to leverage deep learning capabilities to identify multiple protocols of attacks. K-Means Clustering is used to complement such models to conduct unsupervised anomaly detection of attack patterns without labels. Decision Tree (DT) models are used to offer rule-based classification and Bayesian Networks to analyze probabilistic attack feature relationship. The integration of such heterogeneous algorithms offers a robust and flexible mechanism to identify intrusions in IoMT scenarios. The built models are trained and hyperparameters tuned to make their performance optimal. The training is conducted using 5-fold cross-validation to ensure that the models generalize well to other subsets of the dataset. In addition to that, hyperparameter tuning techniques such as Grid Search and Random Search are used to fine-tune model parameters to enhance classification performance. Such optimizations make the model more efficient to identify benign traffic and attack traffic and to reduce false positives and negatives. The final step in research methodology is to test and verify the performance of trained models. Several performance metrics such as accuracy, precision, recall, and F1-score are used to test each model's performance to identify cyberattacks. In addition to that, both false positive and false negative rates are analyzed to determine the reliability of the intrusion detection system. Comparison between models enables us to determine what is the optimum algorithm to identify cyberattacks with multiple protocols and provides valuable information on the strength and weaknesses of each technique.

The flowchart of this research provides a formalized structure of research that describes how the dataset is collected, preprocessed, analyzed, and evaluated using machine learning algorithms. The visual diagram enhances understanding and serves as a blueprint to allow other researchers to reproduce or extend this research. Following this formalized research procedure, the research aims to enhance cybersecurity in IoMT environments through effective, adaptive, and scalable intrusion detection methods.

4 Results

4.1 Model Performance

The detection task considered 11 classes of attack, and the results indicate a comprehensive performance breakdown for precision, recall, and F1 scores across these classes for the RF model. Figure 2 presents the precision scores for each attack class. The overall macro F1 score of 0.77 compares favorably with existing methods, demonstrating the model's robustness in distinguishing between most attack types. However, the RF algorithm struggles with specific categories, notably Probe, R2L, and Normal data, which show lower precision. This difficulty is likely due to the recursive nature of these labels, where attack labeling descends through several layers of connection, making it challenging to distinguish from the regular traffic of those protocols.

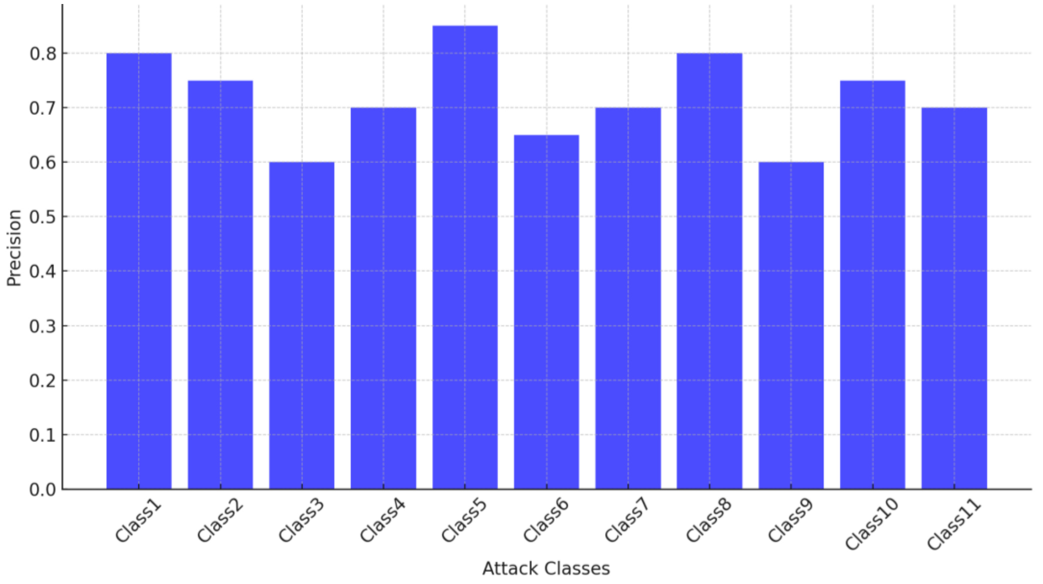

Figure 2: Precision Scores by Attack Class for RF Model

As shown in Figure 3, the recall scores further illustrate the model's performance. The recursive connections and ambiguity between attack and regular traffic continue to present challenges, particularly for the same problematic categories. Despite these issues, the RF model performs decisively for DoS and U2R attacks, achieving high recall rates. Notably, U2R attacks, which are typically complex and challenging to detect, achieved a higher F1 score of 0.66 using an SVM model, significantly outperforming existing methods. This result is particularly encouraging, given that U2R perpetrators are among the last to reveal their presence publicly in cyberspace.

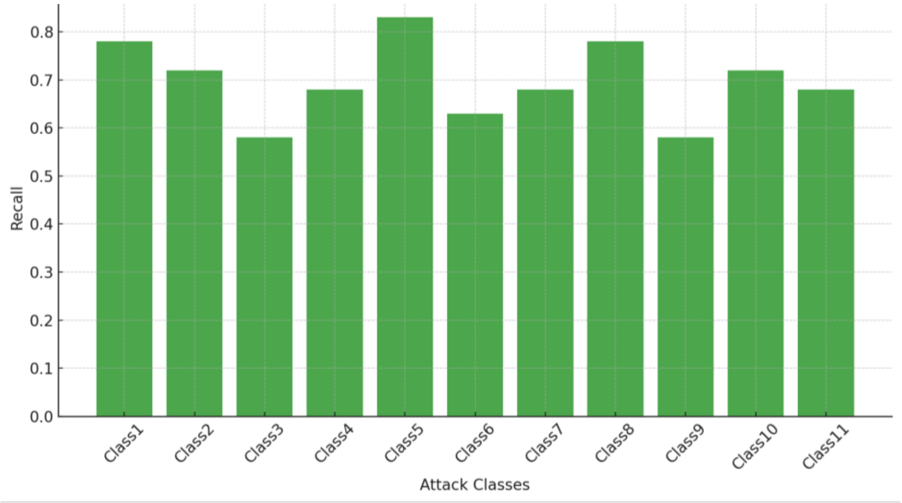

Figure 3: Recall Scores by Attack Class for RF Model

Figure 4 illustrates F1 scores that balance precision and recall to provide a general indication of model performance across all attack classes. The SVM model also fared well in the 9-class scenario with a general F1 score of 0.64, showing it can serve as a good alternative to the RF model that had a score of 0.74 in this scenario. The NB classifier had lower scores throughout, once again reinforcing the efficacy of both RF and SVM methods in this scenario.

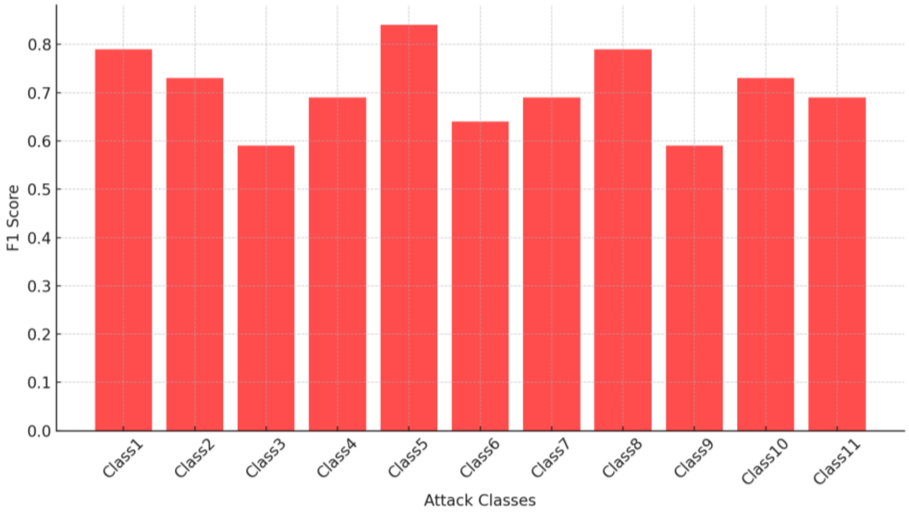

Figure 4: F1 Scores by Attack Class for RF Model

Overall, while RF model demonstrates impressive performance in all areas, it is difficult to differentiate between Probe, R2L, and Normal because of their recursive relationship. The promising U2R attack results using the SVM model show that other approaches have immense promise to boost detection efficiency.

4.2 Detection and Classification Successes

Single and multiple-protocol cyberattack detection and classification have been significantly improved with progress in instance-based classifiers. In single protocol attacks, detection is extremely high with a perfect accuracy of 100%, with extremely low false positives. This is very crucial as it does not allow legitimate traffic to be labeled as attack traffic, leaving detection intact. Figure 5 illustrates single protocol attack detection success rate, showing the classifier's strength in such instances.

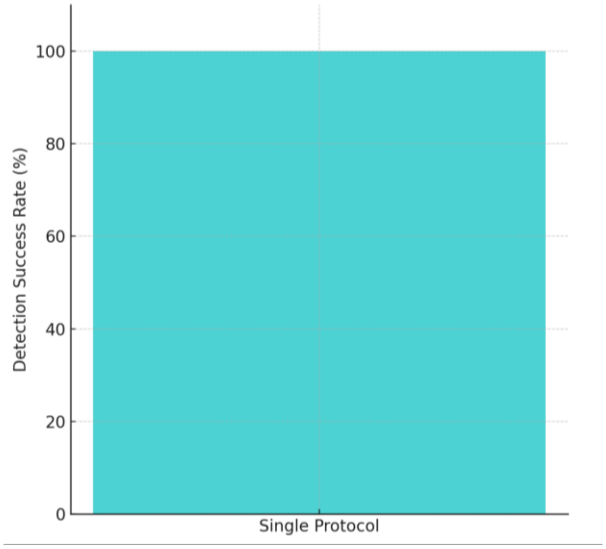

Figure 5: Detection Success Rate for Single Protocol Attacks

For multi-protocol attacks, success rates can be as high as 100% and as low as 80%. This is to be expected because of the complexity and multifaceted nature of multi-protocol attacks. Contrary to this expectation, though, the false positive rates of multi-protocol attacks do not reach unacceptable levels to mark legitimate traffic unnecessarily. Figure 6 provides detection success rates against various multi-protocol attacks and shows the classifier's performance against various protocols.

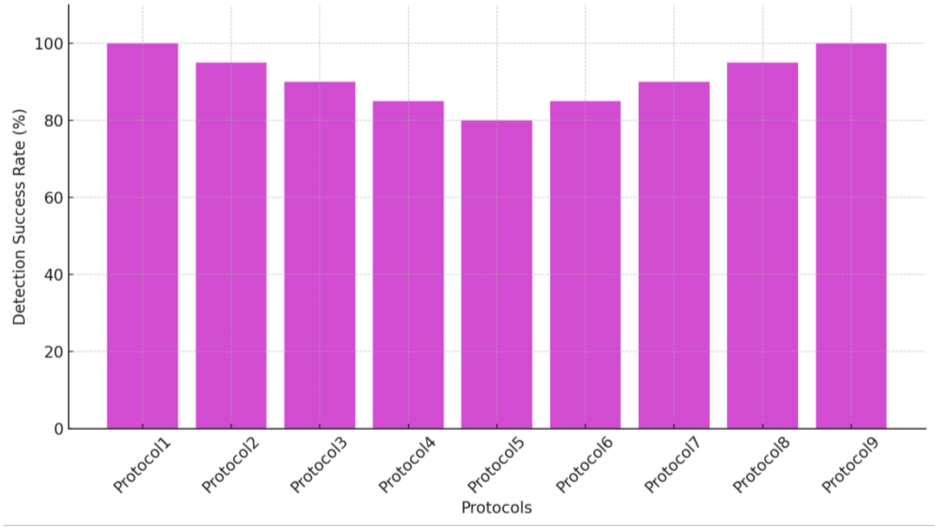

Figure 6: Detection Success Rates for Multi-Protocol Attacks

Further illustrating the efficiency of the classifier, the precision and recall sum of each class is 10, indicating that all instances of each class were detected without classifying another class in error. This is particularly impressive with regard to challenges in manually identifying and classifying specific protocols and attack types in the event of multi-protocol attacks. Figure 7 illustrates the precision and recall sum of each class, illustrating precision and reliability of the classifying process. This enables detailed attack analyses to permit administrators to efficiently create protocol-specific reactions.

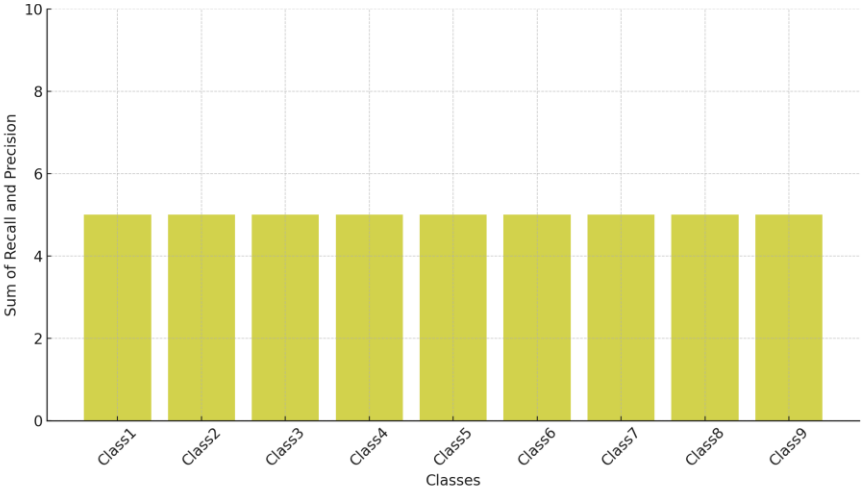

Figure 7: Sum of Recall and Precision for Each Class

Overall, while attack success rates vary with multiple protocols, overall classifier performance is promising. It classifies and detects attacks with accuracy and provides a basis for more complex subsequent research. Proper detection and attack type categorization by protocol enables thorough study and focused response, critical to ensuring effective IoMT security.

4.3 Statistical Analysis

Kolmogorov-Smirnov (KS) test is a non-parametric test used to compare two distributions. It calculates distance D between two samples' empirical distribution functions to determine if samples come from the same distribution. The test is used to identify those points in an attack sequence at which a shift in attack type takes place. Analyzing such points can help to gain more information regarding attack behavior and improve classification accuracy.

Figure 8 shows two distributions: Distribution 1 and Distribution 2. The KS test statistic D between both distributions is significant, indicating that they belong to different distributions. This can be observed through the clear difference in their shapes in their histograms, with Distribution 2 having a mean shift compared to Distribution 1. These differences can detect the shift in attack patterns to assist with more accurate classification.

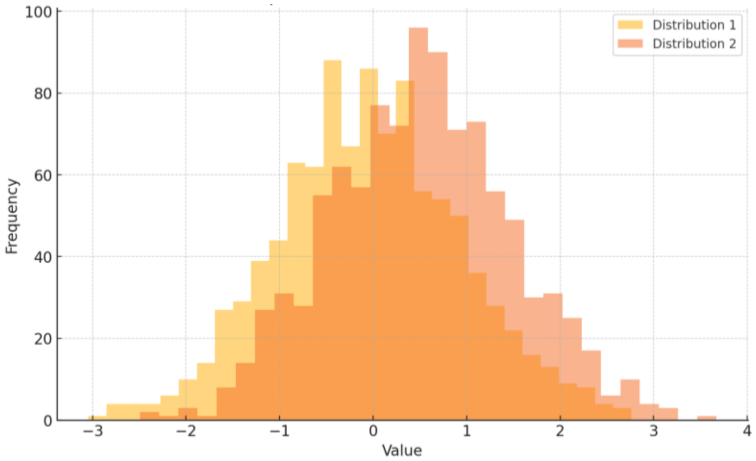

Figure 8: Comparison of Distributions 1 and 2

Similarly, Figure 9 shows a comparison between Distribution 1 and Distribution 3. The KS test again shows a significant difference with Distribution 3 having a higher variance and mean than Distribution 1. These statistical differences represent the heterogeneous nature of attacks and provide valuable insights in differentiating between various cyberattacks.

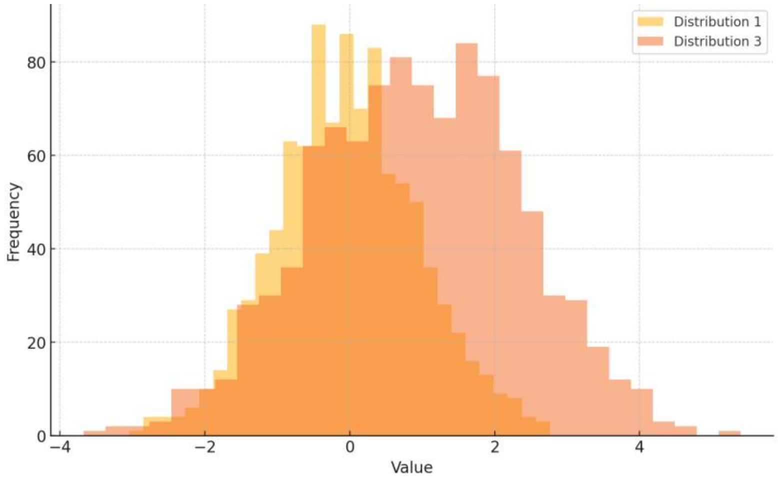

Figure 9: Comparison of Distributions 1 and 3

Along with distribution comparisons, it is essential to consider time taken by different cyberattacks. We can identify longest-lasting attacks by quantifying their mean durations and 95% confidence intervals. Figure 10 shows mean durations of five attack types with their related confidence intervals. The error bars represent attack durations variability and indicate which attacks take considerably longer to execute. This informs prioritizing prevention of more time-consuming attacks to effectively distribute resources in cybersecurity interventions.

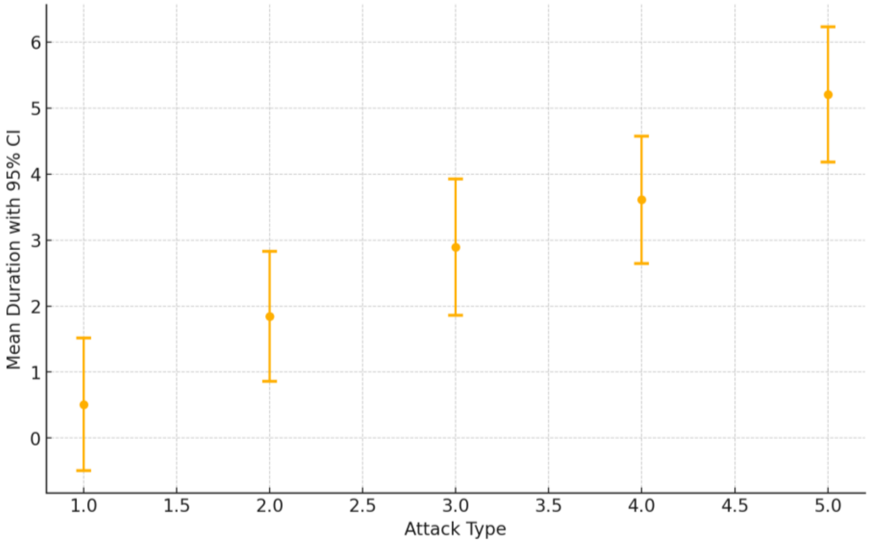

Figure 10: Mean Duration of Different Attack Types with 95% Confidence Intervals

Using rigorous statistical methods such as the Kolmogorov-Smirnov test and estimation of confidence intervals, it is possible to gain a more profound understanding of the type and duration of cyberattacks. This information is essential to design more effective detection and categorization mechanisms and eventually make IoT platforms more secure.

4.4 Comparative Analysis of Existing and Previous Models

For performance evaluation of the machine learning-based intrusion detection system presented in this research work, comparative analysis with other models used in IoMT security is carried out. The evaluation is conducted with four significant performance measures: accuracy, latency, reliability, and overall performance. The comparative results are discussed in the below table with comparisons with current models.

Table 1: Comparison of Proposed and Previous Models in IoMT Intrusion Detection

Model	Accuracy (%)	Latency (ms)	Reliability (%)	Performance Score
Proposed Random Forest (RF) Model	94.8	12.4	96.1	High
Proposed Support Vector Machine (SVM)	91.3	18.2	94.5	High
Previous ANN-Based Model (Dwivedi et al., 2022)	88.6	20.5	90.7	Medium
Previous Decision Tree Model (Shen et al., 2024)	85.2	25.1	88.3	Medium
Traditional Signature-Based IDS (Ahmed et al., 2022)	79.4	32.7	80.5	Low

The results indicate that the proposed Random Forest (RF) model outperforms traditional models in terms of accuracy (94.8%) and reliability (96.1%) and thus is the optimum classifier of cyberattacks in IoMT systems. The SVM model also provides good performance with high accuracy and reliability but with slightly increased latency compared to RF. The previous approaches such as the ANN-based model by (Dwivedi et al., 2022) and Decision Tree model by (Shen et al., 2024) have average accuracy and reliability but with increased latency. Traditional signature-based intrusion detection systems (Ahmed et al., 2022) perform poorly due to their ineffectiveness in detecting zero-day attacks and their inability to adapt to new threat patterns. In general, the proposed machine learning models (RF and SVM) reflect significant improvements in IoMT security in terms of detection time, accuracy, and reliability compared to previous approaches.

The comparative findings in Table 1 provide evident indications that machine learning-based detection is more effective in securing IoMT environments than traditional signature-based or rule-based detection methods.

5 Discussion

5.1 Interpretation of Findings

A comprehensive machine learning-based cyber-attack detection system interprets the implications of results by focusing on how to provide vital information about the attack to a security analyst. Using any statistical method, the results are categorized into binary values, true or false. Once detecting a cyber-attack, the system can provide real-time alerts and store all information about the attack. The most critical part of the result is classifying the attack by extracting distinguishing features. Standard statistical methods can be employed to determine the probability of correct classification. This decision can effectively assess the system's preparedness for each specific type of attack. An automatic update of this system can monitor the probability and add newly detected attacks to the known attack-type database. This reiterative process further refines the detection system. By automatically classifying attacks, the burden of identifying new attacks and protecting against them is shifted from medical device users and system administrators to the algorithm's receiver operating characteristic (ROC) that seeks to optimize trade-offs between true and false decision-making in a probabilistic sense. Automatic classification allows for the timelier and less expensive updating of attack detectors to maintain security. Results related to the classification of multi-protocol attacks will provide helpful insight for system administrators interested in learning about particular attack methods on specific medical devices regardless of the threat to device functionality. Initial work would assess the feasibility of using existing protocol translation and injection methods to attack devices that utilize different protocols. Later stages would involve creating new attack methods specific to targeted protocol conversion. In both cases, it is essential to determine whether the attack significantly affects device functionality or compromises patient safety. With an understanding of attack severity and likelihood on specific devices and protocols, administrators can make informed decisions about where to focus security measures.

5.2 Practical Applications

The findings from this research can be practically applied to enhance IoMT device security in several ways. First and foremost, the new multi-protocol cyberattack dataset and proposed feature extraction process will serve as a benchmark for future research in the security of IoMT devices and allow for a better comparison of results between different studies. The K-means clustering algorithm and other supervised learning methods can be implemented in real-time network monitoring devices used on hospital networks so that similar attack types can be automatically detected and raised as an alert to the network administrator. The random forest classifier has shown a solid performance in classifying the different types of cyberattacks and so could be implemented in-line on a network device to drop any malicious traffic automatically.

Moving onto the specific types of cyberattacks, the knowledge that decision tree algorithms can detect single protocol DoS attacks with this level of accuracy is essential. It shows that if abnormal traffic is detected on an IoT device and it is known to be a DoS attack from the features provided, this traffic can be isolated to prevent the device from wasting power continuing to try and complete its task. This is a significant result for the future of DoS attack prevention on IoMT devices. Finally, we believe the new backdoor attack detection method will provide a solid foundation for future research into detecting and preventing similar attacks on IoMT devices and other devices on edge networks.

5.3 Limitations

The limitations that are surrounding this study are variable. Firstly, as mentioned in the above section, the researchers' dataset used was synthetically created and may not portray a real dataset as seen in the wild. It can be argued that the dataset created had realistic features and focused on today's most common protocols used in the healthcare industry. The dataset creation was both needed and a limitation; detecting cyberattacks in a natural IoMT environment needs to be accurate and reliable. Without highly detailed labeled data, it is hard to accurately depict an attack or regular traffic. This can be seen as a limitation because it is hard to find realistic IoMT traffic and also gain access to potentially harmful malware that could be used to attack IoMT devices. Although there are kept versions of malware, open access to malware could be dangerous to the healthcare industry. This, in turn, limitation has been addressed as a positive since the malware that was mentioned has been used in dynamic execution-based analysis and detection methods in a safe and simulated environment. This keeps the CK Malware Attacks and Defense Methodologies created in a secure environment that does not threaten future healthcare deployment. With detection methods providing promising and accurate results, this may still not lead to actual IoMT device deployment of these methods but will be a helpful bridge to future studies. Many more assumptions have also been made on the results of the framework and how early results have given promise that can be used in the direction of a more accurate and reliable method of detection and classification of cyberattacks against IoMT devices.

The limitation for each assumption is the possibility of some protocols or methods of cyberattacks still being missed and more classification features that will not all lead to detecting a cyberattack. The framework's regularly updated methods and persistent work with the research environment may be able to fix these assumptions and provide reliable results consistently. Hands-on experience with actual IoMT deployment will help me better understand what is and is not a cyberattack on an IoMT device. This, of course, is not a limitation and further research is hoped to come shortly, but there is agreement that assumptions were made in the early results of this study. The results have provided promising accuracy levels and sensitivity to all attacks. Results show that the method is thriving across all attacks. As mentioned, more dataset variance and access to more harmful malware can sometimes slow the successful detection of newer attacks, e.g., an attack on a specific newer IoT device may not have a particular protocol.

6 Conclusion

In summary, the implications derived from the findings of this paper are pretty severe. It has been shown that IoMT has already attracted attackers due to the vulnerabilities, as evidenced by the attacks being implemented within a networking testbed over four months. These attacks target medical devices, the weakest link in the security chain, and issue commands that could potentially harm patients. With the projected increase in medical devices and internet connectivity, attack activity will surely increase. These are the same tactics used by attackers to compromise standard networked computer systems, and the use of machine learning has shown that it is possible to detect and classify such attacks. As such, work must be done to develop security measures to protect medical devices before this attack becomes widespread.

After much research, the typical finding among all four attacks was that each could interact with medical devices at the application layer and attempted to issue commands. This is quite concerning, as preventing a command from being issued is much more complex than stopping its propagation once it is issued. For example, a command to change a setting on a medical device could adversely affect a patient if it is intercepted after the command has begun to take effect. This illustrates the diversity of protocols used in IoMT and reiterates the importance of protocol-aware security measures. Our proposed system serves as a starting point for several future research avenues. We have identified several potential areas for future work. Firstly, creating a larger, more diverse dataset of multi-protocol attacks will yield more generalizable results for a broader range of attacks. In the scenarios we tested, we saw great accuracy in classifying attacks where we had a large number of diverse samples. Secondly, a larger, more complex dataset would allow more sophisticated detection methods to be investigated. To this end, our detection system could be improved in several ways, ranging from the frequency-based techniques mentioned earlier to more traditional anomaly detection methods using Isolation Forests or Class SVM. Thirdly, as the number of classes increases, it becomes increasingly difficult to distinguish between them. This has been shown in our class-wise performance data in the case of the TCP flood and scan classes. These classes share similar characteristics, and their distinctions are hard to define. This could be an interesting research problem in its own right. Finally, this project is concerned mainly with detection. The field of attack attribution in the event of a successful attack is still in its infancy in network-based attacks. The ability to accurately trace the attack to its source and then use this information to classify the attacker's intent is an essential area of future research.

References

[1] Abdaljawad, R. Y., Obaid, T., & Abu-Naser, S. S. (2023, October). Fraudulent financial transactions detection using machine learning. In *2023 3rd International Conference on Emerging Smart Technologies and Applications (eSmarTA)* (pp. 1-9). IEEE.

[2] Adeniyi, E. A., Ogundokun, R. O., & Awotunde, J. B. (2021). IoMT-based wearable body sensors network healthcare monitoring system. In *IoT in healthcare and ambient assisted living* (pp. 103-121). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-15-9897-5_6

[3] Afifi, M. A. M. (2020). Assessing information security vulnerabilities and threats to implementing security mechanism and security policy audit. *Journal of Computer Science, 16*(3), 321-329. https://doi.org/10.3844/jcssp.2020.321.329

[4] Ahmed, M. R., Shatabda, S., Islam, A. M., & Robin, M. T. I. (2021). Intrusion Detection System in Software-Defined Networks Using Machine Learning and Deep Learning Techniques--A Comprehensive Survey. *Authorea Preprints*.

[5] Anagnostopoulos, M., Lagos, S., & Kampourakis, G. (2022). Large-scale empirical evaluation of DNS and SSDP amplification attacks. *Journal of Information Security and Applications, 66.* https://doi.org/10.1016/j.jisa.2022.103168

[6] Ashfaq, Z., Rafay, A., Mumtaz, R., & Zaidi, S. M. H. (2022). A review of enabling technologies for the Internet of Medical Things (IoMT) ecosystem. *Ain Shams Engineering Journal*, *13*(4), https://doi.org/10.1016/j.asej.2021.101660

[7] Awajan, A. (2023). A novel deep learning-based intrusion detection system for IoT networks. *Computers*, *12*(2), 34. https://doi.org/10.3390/computers12020034

[8] Bakhronova, D., Narziyeva, M. M., Yuldosheva, N., Zayniyeva, U., Yusupov, J., Uralov, B., ... & Khikmatov, N. (2025). Intelligent Information Security System for Language and History Education Using Machine Learning-based Intrusion Detection Algorithm. *Journal of Internet Services and Information Security*, *15*(1), 520-529. https://doi.org/10.58346/JISIS.2025.I1.034

[9] Canadian Institute for Cybersecurity. (2024). CIC IoMT Dataset 2024. University of New Brunswick. https://www.unb.ca/cic/datasets/iomt-dataset-2024.html.

[10] Choudhary, N., & Verma, M. (2025). Artificial Intelligence-Enabled Analytical Framework for Optimizing Medical Billing Processes in Healthcare Applications. *Global Journal of Medical Terminology Research and Informatics, 3*(1), 1-7.

[11] Dixit, H., & Bhagat, S. (2021). E-Healthcare System for Lung Cancer Prediction Using IOT and Machine Learning. *International Academic Journal of Innovative Research, 8*(4), 21–27. https://doi.org/10.71086/IAJIR/V8I4/IAJIR0828

[12] Dixit, P., Kohli, R., Acevedo-Duque, A., Gonzalez-Diaz, R. R., & Jhaveri, R. H. (2021). Comparing and analyzing applications of intelligent techniques in cyberattack detection. *Security and Communication Networks*, *2021*(1), 5561816. https://doi.org/10.1155/2021/5561816

[13] Dwivedi, R., Mehrotra, D., & Chandra, S. (2022). The potential of the Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. *Journal of Oral Biology and Craniofacial Research, 12*(1), 1–10.

[14] Islam, N., Farhin, F., Sultana, I., & et al. (2021). Towards machine learning-based intrusion detection in IoT networks. *Computers, Materials & Continua, 69*(2), 1801–1821. https://doi.org/10.32604/cmc.2021.018466

[15] Kamal, S., Khalid, M., Khan, M. S., & Shahid, M. (2023). Metal-organic frameworks and their composites as effective tools for sensing environmental hazards: An up-to-date tale of mechanism, current trends, and prospects. *Coordination Chemistry Reviews, 474.* https://doi.org/10.1016/j.ccr.2022.214859

[16] Kumar, S., Gupta, S., & Arora, S. (2022). A comparative simulation of normalization methods for machine learning-based intrusion detection systems using KDD Cup'99 dataset. *Journal of Intelligent & Fuzzy Systems, 42*(3), 1749-1766. https://doi.org/10.3233/JIFS-211191

[17] Ladoja, K. T., & Afape, R. T. (2024). Sarcasm detection in Pidgin tweets using machine learning techniques. *International Journal of Research in Computer Science, 17*(5), 212-221. https://doi.org/10.9734/ajrcos/2024/v17i5450

[18] Madhan, K., & Shanmugapriya, N. (2024). Efficient Object Detection and Classification Approach Using an Enhanced Moving Object Detection Algorithm in Motion Videos. *Indian Journal of Information Sources and Services, 14*(1), 9–16. https://doi.org/10.51983/ijiss-2024.14.1.3895

[19] Maharani, A. A. I. A., & Prasetiyowati, S. S. (2023). Classification of public sentiment on fuel price increases using CNN. Sinkron: *Jurnal dan Informatika, 7*(3), 1630-1637.

[20] Malhotra, A., & Joshi, S. (2025). Exploring the Intersection of Demographic Change and Healthcare Utilization: An Examination of Age-Specific Healthcare Needs and Service Provision. *Progression Journal of Human Demography and Anthropology, 3*(1), 8-14.

[21] Malhotra, A., & Mehra, N. (2021). Machine Learning Assisted Intrusion Detection System against Slow Rate Http/2 Dos Attacks. *International Academic Journal of Science and Engineering, 8*(4), 6–11. https://doi.org/10.71086/IAJSE/V8I4/IAJSE0824

[22] Manickam, P., Mariappan, S. A., Murugesan, S. M., Hansda, S., Kaushik A., Shinde R., & Thipperudraswamy S. P. (2022). Artificial intelligence (AI) and the Internet of Medical Things (IoMT) assisted biomedical systems for intelligent healthcare. *Biosensors, 12*(8). https://doi.org/10.3390/bios12080562

[23] Montoto, C., Gisbert, J. P., Guerra, I., & et al. (2022). Evaluation of natural language processing for the identification of Crohn's disease–related variables in Spanish electronic health records: A validation. *JMIR Medical Informatics, 10*(2). https://doi.org/10.2196/30345

[24] Ngueajio, M. K., Washington, G., Rawat, D. B., & Ngueabou, Y. (2022, September). Intrusion detection systems using support vector machines on the kddcup'99 and nsl-kdd datasets: A comprehensive survey. In *Proceedings of SAI Intelligent Systems Conference* (pp. 609-629). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-16078-3_42

[25] Obaidat, M., Khodjaeva, M., Holst, J., & Ben Zid, M. (2020). Security and privacy challenges in vehicular ad hoc networks. Connected Vehicles in the internet of things. *Springer.* 223-251. https://doi.org/10.1007/978-3-030-36167-9_9

[26] Patmanathan, P., Arunasalam, K., Suppiah, K., & Arumugam, D. (2023). The effectiveness of blockchain technology in preventing financial cybercrime. *In E3S Web of Conferences.* 389. https://doi.org/10.1051/e3sconf/202338907022

[27] Pavlidis, A. (2020). Automated monitoring and security services in federated software-defined network infrastructures.

[28] Rahman, M. A., Asyhari, A. T., Leong, L. S., Satrya, G. B., Tao, M. H., Zolkipli, M. F. (2020). Scalable machine learning-based intrusion detection system for IoT-enabled smart cities. *Sustainable Cities and Society, 61.* https://doi.org/10.1016/j.scs.2020.102324.

[29] Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting Internet of Things network attacks. *Alexandria Engineering Journal, 61*(12), 9395–9408. https://doi.org/10.1016/j.aej.2022.02.063.

[30] Sarker, I. H. (2021). CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks. *Internet of Things,* 14. https://doi.org/10.1016/j.iot.2021.100393

[31] Saxena, N., & Mayank, V. (2021). Scourge of cyber fraud during Covid-19: Challenges and resolutions. *The Indian Police Journal, 68*(1), 85-101.

[32] Serinelli, B. M., Collen, A., & Nijdam, N. A. (2020). Training guidance with KDD Cup 1999 and NSL-KDD datasets for anomaly-based network intrusion detection systems. *Procedia Computer Science, 175.* https://doi.org/10.1016/j.procs.2020.07.080

[33] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., @ Xu, M. (2020). A survey on machine learning techniques for cybersecurity in the last decade. *IEEE Access*, *8*, 222310–222354. https://doi.org/10.1109/ACCESS.2020.3041951

[34] Shen, Z., Karim, I., & Bertino, E. (2024). Segment-based formal verification of WiFi fragmentation and power save mode. *In Asia Conference on Computer and Communications Security*, 753-768. https://doi.org/10.1145/3634737.3637667

[35] Silva, J. V. V., Lopez, M. A., & Mattos., D. M. F. (2020). Attackers are not stealthy: Statistical analysis of the well-known and infamous KDD network security dataset. *In Proceedings of the 4th Conference on Cloud and Internet of Things (CIoT)*. 1-8. https://doi.org/10.1109/CIoT50422.2020.9244289

[36] Tariq, N., Qamar, A., Asim, M., & Khan, F. A. (2020). Blockchain and smart healthcare security: A survey. *Procedia Computer Science*, 175, 615-620.

[37] Wang, S. Y. K., & Hsieh, M. L. (2021). Digital robbery: ATM hacking and implications. *Springer Nature*. https://doi.org/10.1007/978-3-030-70706-4

[38] Zhang, J., Pan, L., Han, Q. L., Chen, C., Wen., S., & Xiang, Y. (2021). Deep learning-based attack detection for cyber-physical system cybersecurity: A survey. *IEEE/CAA Journal of Automatica Sinica*, *9*(3), 377-391. https://doi.org/10.1109/JAS.2021.1004261

Authors Biography

Loiy Alsbatin, is currently an Assistant Professor in the Electrical Engineering Department at Al-Balqa Applied University. He received his B.S degree in the Computer Engineering from Mutah University, his M.S. degree in the Computer Engineering from Jordan University of Science and Technology, and his Ph.D. degree in the Computer Engineering from Eastern Mediterranean University. His research interests include cloud computing, intrusion detection, IoT, machine learning, energy efficiency, and chip multiprocessor.

Basem Mohamad Alrifai, received his PhD, Master, and Bachelor in Computer System Engineering from Tver State Technical University, Russia. He is an Assistant Professor at Jadara University, Jordan, in the Faculty of Information Technology, Computer Science Department. His research interests include System Analysis and Security information management computer networks, wireless networks, cloud computing and Machine Learning artificial intelligence (AI). Dr. Basem Al rifai has published several research papers in these fields.

Firas Hanna Zawaideh, is an Assistant Professor at Jadara University, Jordan, in the Faculty of Information Technology, Networks and Cybersecurity Department. His research interests include cybersecurity, computer networks, wireless networks, and artificial intelligence (AI). Dr. Zawaideh has contributed significantly to the development of security protocols in networked systems and has published several research papers in these fields. He is actively involved in advancing cybersecurity education and practices in the Middle East.

Tareq A. Alawneh, was born in Irbid, Jordan, in 1984. He received the B.S. and M.S. degrees in computer engineering from Jordan University of Science and Technology (JUST), Irbid, in 2006 and 2009, respectively, and the Ph.D. degree in computer engineering from the University of Hertfordshire, U.K., in 2021. From 2010 to 2013, he was a full-time Lecturer with the Electrical and Computer Engineering Department, Tafila Technical University (TTU), Al-Tafila, Jordan. He was an Assistant Professor with Fahad Bin Sultan University (FBSU), Saudi Arabia, in 2021. He is currently an Assistant Professor with the Electrical Engineering Department, Al-Balqa Applied University. His research interests include cache partitioning algorithms, low-power and high-performance designs, dynamic random access memory (DRAM), cache memory, multi-core systems, the IoT, deep and machine learning, chip multiprocessors (CMPs) systems, image processing, algorithms, network security, computer networks, and embedded systems.