Enhancing Security of IoT Enabled Smart Healthcare Clinics Using MUD

Vaishali Soni, Deepika Kukreja* and Amarjit Malhotra

Netaji Subhas University of Technology, Dwarka, Delhi, India
E-mail: deepika.kukreja@nsut.ac.in
**Corresponding Author*

Received 08 January 2025; Accepted 01 May 2025

Abstract

The rapid adoption of the Internet of Things (IoT) is changing almost all aspects of life and the use of these technologies is increasing in different sectors such as education, healthcare and manufacturing. Within the healthcare sector, smart clinics are coming up as new generation of healthcare facilities connected with IoT-enabled medical devices like cameras, diagnostic devices and sensors to aid in patient care. However, this paper has established that security is a major concern in the use of IoT devices due to the fact that most of them are unprotected and therefore prone to attacks. In response to this problem, the Internet Engineering Task Force (IETF) suggested the Manufacturer Usage Description (MUD) framework to specify safe communication behaviors for IoT devices. This paper proposes the adoption of MUD profiling to improve the security position of IoT powered smart clinics. When MUD profiles were applied to devices in the ECU-IoHT dataset, we were able to get a better anomaly detection using Machine Learning (ML) models. Random Forest and XGBoost classifiers had a gain in accuracy of 1.43% and 1.74% respectively, MLP increased by 2.80% and CatBoost increased by 0.51%. These results show that MUD based security mechanisms can be useful in protecting IoT based healthcare environments.

Keywords: Smart healthcare, smart clinics, manufacturer usage description (MUD), security, internet of healthcare things, ECU-IOHT dataset.

Journal of Mobile Multimedia, Vol. 21_3&4, 633–660.
doi: 10.13052/jmm1550-4646.213417

1 Introduction

The Internet of Things (IoT) has recently come into its own as an important technology across a number of sectors, including healthcare, where it has been one of the most affected industries. IoT has been adopted in the healthcare sector to develop smart clinics equipped with connected devices like patient monitoring sensors, surveillance cameras and diagnostic equipment. However, the realization of these innovations has been accompanied by major security risks. Most IoT medical devices are insecure by design, posing a risk of exploitation through cyber attacks. These issues are important because they threaten patient safety, data integrity, and operational reliability.

The growing interconnectedness of healthcare devices has resulted in an uptick of cyberattacks on IoT infrastructures. Many IoT medical devices are equipped with limited security features that make them easy to hack and access. The Gartner report says cyber attacks on operational technology (OT) environments will increase significantly and threaten critical infrastructures by 2025 [1]. The SonicWall Mid-Year Threat Report 2024 also showed a 107% increase in IoT-based cyber attacks, which highlights the need to deploy better security measures [2].

IoT devices works on top of existing protocols like Bluetooth, Wi-Fi, and Zigbee for smooth connectivity. But that's also opened up the attack surface, since many of these devices are insecure right out of the box. With default passwords, insecure firmware, and poorly isolated networks, they are a major attractor for attackers. Many of these devices are bare bone when it comes to security controls, and that has greatly ascribed to the attack surface.

As per the SonicWall Mid-Year Threat Report of 2024, there has been a 107% rise in IoT targeted attacks in the first half of the year and this shows that there is a great need to enhance the IoT security solutions [2]. This sharp rise shows that attackers are now more likely to go after IoT devices than ever before, and this is probably because they are easier to hack being weak in security.

So that attackers cannot use IoT devices as 'low hanging fruits', security has to be done in the network. IoT devices should be secure for themselves but being resource constrained they are incapable of achieving this. Hence security at network level is required. Securing the routing protocols is a good way to enhance network security [3, 4] to the best of our knowledge.

The disclosure of a patient's information is usually a major issue of concern in the health care sector. Even a simple interception attack can open the door to more severe threats like malware injection. The use of default

passwords in medical IoT devices is a major vulnerability in smart clinic environments that can be exploited to gain unauthorized access to the network and cause a lot of damage [5].

To enhance the security of IoT installations, the Internet Engineering Task Force (IETF) suggested the Manufacturer Usage Description (MUD) framework. The purpose of MUD is to assist device manufacturers to define the normal communications that a device should have with the network and for the network administrators to enforce them, thus reducing the chances of unauthorized or malicious activities [6]. Hence, MUD offers a way of limiting unauthorized or anomalous traffic, thus being a good way of defending against cyber attacks to enhance the reliability and security of IoT networks [7].

MUD can be used to explain the expected behaviour of an IoT device in certain ways, in terms of specific communication policies [8]. This ensures that any unapproved activity is not performed by the device since all communication is being watched [9]. In this way, the restricted communication features and the legitimate uses of IoT devices can be put to the development of good security policies on network devices like switches and routers [10].

The idea of MUD standards are a good concept and are based on the concept of defining the expected communication behaviors of IoT devices. MUD profiles are not enough to solve the problem of the dynamic nature of cyber threats. These profiles are static and predefined that makes them failure in real time to mimic new attack patterns. This gap leads to the burning question of the need for more adaptable security solutions that can detect and respond to threats as they emerge especially in critical areas such as healthcare where the costs of breaches are high.

Today's security solutions for IoT networks are based either on static, predefined policies – for instance, those enabled by MUD profiles – or on dynamic anomaly detection with the help of Machine Learning (ML). However, there are some disadvantages of both approaches. MUD profiles are practical in constraining the normal operation of devices but are static and incapable of accommodating the dynamic communication phenomena which are characteristic of healthcare environments. However, standalone ML models are good at anomaly detection but have high false positive rates, especially in healthcare where device interactions are strenuous and vital.

This paper proposes a hybrid approach of integrating MUD based predefined behavioral profiles with ML models to enhance the detection accuracy and reduce false positives in real-time for healthcare IoT environments as it faces challenges of device richness, patient data sensitivity and service

continuity requirements. The key aim of this research is to design a solution that can help minimize the occurrence of false positives in anomaly detection models, thus increasing the reliability and efficiency of the detection process in healthcare environments.

1.1 Research Gap

While previous studies have explored the application of MUD in securing IoT networks, few have combined this approach with Machine Learning models to enhance anomaly detection capabilities. Existing research primarily focuses on either using MUD for static policy enforcement or employing Machine Learning for dynamic intrusion detection, but the integration of these two approaches has not been thoroughly explored, especially in the context of healthcare IoT systems.

This research tries to bridge this gap through a novel method that combines MUD profiling with Machine Learning algorithms to enhance the real-time detection and classification of network anomalies in IoT-enabled healthcare clinics.

1.2 Study Objectives and Contributions

In this research, we propose the application of MUD profiling to improve the security of IoT-enabled smart healthcare environments. Thus, by creating MUD profiles for every device, we can identify typical communication patterns that can be used as a reference point when identifying suspicious behavior. Then, the machine learning models are trained to detect anomalies, i.e., deviations from the learned communication patterns, which can help to detect potential security threats in the network in real-time.

We specifically assess the effectiveness of applying MUD profiles to healthcare-related IoT systems using the ECU-IoHT dataset of Edith Cowan University [11]. The study investigates the effectiveness of integrating MUD with machine learning algorithms such as Random Forest, MLP, XGBoost, and CatBoost to enhance the detection and classification of network anomalies. The results indicate that the integration of MUD enhances the performance of these models in identifying abnormal activities.

- Adding MUD profiling to each device in the Edith Cowan University-Internet of Health Things (ECU-IoHT) dataset [11].
- Evaluating how well the Intrusion Detection System (IDS) performs after including MUD profiling.

- Comparing the performance of different Machine Learning models such as XGBoost, CatBoost, Random Forest and Multilayer Perceptron (MLP).

2 Related Work

With more IoT devices being deployed and more risks that come with it, securing these systems has thus become an important issue [12]. The MUD standard was developed to improve the security of IoT devices by defining what a normal operating condition of a device is in terms of the communications it is expected to make, which enforces the communication within allowed paths and therefore protects against bad practices. Many works have employed the MUD profiling for different IoT security scenarios.

In their work, Heeb et al. [13] suggested employing MUD profiles in combination with machine learning techniques to enhance anomaly detection in IoT networks. Their hybrid approach employed deep autoencoders with random forest classifiers to identify variations in the network traffic and gained superior improvement in the accuracy of intrusion detection. To this end, the authors suggested employing MUD profiles as a normal device behavior reference, which in turn reduced the number of false positives and increased security in IoT environments.

To enhance the use of Intrusion Detection Systems (IDS) in IoT environments, Machine Learning (ML) and Deep Learning (DL) techniques are employed. In this paper, Xu et al. [14] suggested that anomaly detection models can be trained on normal traffic to detect suspicious network activities.

Similarly, Alsoufi et al. in [15] pointed out that deep learning models are suitable for large scale and complex datasets for the detection of complicated cyber threats.

To improve the anomaly detection accuracy, Yasaei et al. [16] proposed the model IoT-GRAF that uses graph learning and multi-modal data fusion.

In their work, Imad et al. [17] compared various techniques and stated that improved versions of ML increase the detection rates of different attack types in IoT networks.

Baich et al. [18] also pointed out that ML-based intrusion detection systems are better than the conventional security mechanisms and are a mandatory requirement to protect IoT networks.

The real-world implementation of MUD profiling has been studied in works including the research by Lastdrager et al. [19], in which the authors

proposed SPIN (Security and Privacy for In-home Networks). SPIN complements privacy management applications and reverse firewalls that employ MUD policies to form a safe and customizable in-home network. This paper described how MUD could be applied in practice to stop threats in residential IoT networks.

As IoT systems get larger, secure communication of devices is crucial to manage. Previous studies show how MUD can be used to fight cyber threats and enhance IoT security. Morgese in [20] proposed MUDscope, a tool to help in the analysis of network traffic using MUD profiles to identify and counter threat. Using MUD policies as a reference, MUDscope aggregates rejected network packets into similar clusters and generates valuable threat intelligence from it.

A similar concept was also described by Wannigama et al. [21], who proposed a different implementation of MUDscope to analyze IoT security risks. Their results supported the effectiveness of using MUD profiles in identifying and isolating unauthorized network traffic, thus validating the potential of MUD-based monitoring.

Attacks on IoT devices have been on the rise and MUD has been found to play a crucial role in reducing the attack surface of these devices through the use of defined communication patterns. Heeb et al. [13] explained that MUD manages the device relations to prevent DDoS attacks and unauthorized data leakage. However, they noted that MUD has some weaknesses, including susceptibility to spoofing and the need for robust authentication mechanisms. Although MUD profiles offer a more systematic way of securing devices, they have a major drawback of being unable to cope well with the dynamics present in IoT environments. Previous research has widely applied MUD in the context of IoT network security [13, 20] and the application of ML models for anomaly detection [14, 15]. But, these approaches have some major constraints in healthcare environments. MUD by itself is inert to the changes in device behaviors, whereas the conventional IDS based on the ML model is prone to a large number of false positives because of the intricacy of the traffic in the healthcare network. This demands a combination of MUD profiling and ML to increase the accuracy and toughness of the detection system.

The integration of MUD into IoT security frameworks has been studied in several papers. In [22], Matheu García et al. described how MUD can be integrated into the cyber-physical system model to develop structured security frameworks that describe the expected behavior of a device. Hamza et al. [23] highlighted the significance of developing, validating, and

enforcing behavioural profiles of IoT devices based on MUD to enhance anomaly detection through controlled device communication. In their subsequent paper [24], they explained how the SDN monitoring of MUD can help in identifying volumetric attacks and enhance the current security mechanisms. In [25], De Keersmaeker et al. suggested a profile-based firewall for smart homes and how MUD-based supervision improves the security of devices and prevents unauthorized data communication.

Despite these advancements, research is primarily focused on generalized IoT environments rather than sector specific applications like healthcare. Furthermore, existing studies primarily focus on either MUD or ML based security, and do not aim to explore the potential of their combination. This gap is bridged by our research which integrates MUD profiling with machine learning algorithms to secure IoT enabled healthcare clinics and achieves better security performance using real world data from the ECU-IoHT dataset.

In this paper, we design a new security framework for IoT enabled healthcare clinics which combines MUD profiling together with a machine learning based anomaly detection to increase the overall security of the system. The proposed framework uses MUD to set up a reference model of typical network traffic and uses machine learning to detect any new flows that are not consistent with the model, thus detecting suspicious traffic. This approach not only improves the accuracy of intrusion detection but also strengthens the robustness of the security framework against new threats.

The security of IoT systems is enhanced by the application of MUD in conjunction with anomaly detection based on ML. This combined strategy increases the sensitivity of intrusion detection and at the same time provides a structured and adaptive security structure for IoT ecosystems.

3 Motivation

The application of IoT devices in the healthcare sector has changed the way of patient monitoring and diagnosis and has greatly enhanced the delivery of medical services. But this reliance on the IoT technology has also uncovered some critical security risks. Normal IT systems are different from such devices as IoT devices function with limited computational resources hence it is difficult to embed strong security features. This is particularly a challenge in the healthcare sector where the data is very sensitive and any security breach may have severe implications including legal consequences and loss of patients' trust. Wearable smart devices, patient monitors, and diagnostic

equipment and smart sensors are medical IoT devices that help in managing and monitoring of health care facilities and patient care in real time. However, for this reason, they are more vulnerable to cyber attacks than ever before. Recent research shows that cyber attacks on IoT based healthcare systems are on the rise and the impacts of which may include risks to patient safety and reliability of critical medical infrastructure. These increasing threats have therefore called for the need to strengthen the security mechanisms of IoT based healthcare environments.

Conventional cybersecurity measures are failing for IoT networks due to the heterogeneity and resource constraints of connected devices. Current security protocols, which were developed for general-purpose computing environments, are not well suited to the specificities of IoT ecosystems. To this end, the Internet Engineering Task Force (IETF) proposed the Manufacturer Usage Description (MUD) framework to define the expected communication behaviors of IoT devices. Thus, for example, healthcare managers can restrict the device interactions to certain patterns through MUD profiles – which in turn helps to avoid unauthorized access and misuses. The use of MUD in the healthcare IoT environments has been observed to be efficient in the protection of communication by setting up strong policies [14–16]. However, as the IoT infrastructure is further developed and intensified, MUD may not be enough to block new cyber threats.

Various research efforts have delved into the utilization of MUD in conjunction with other security technologies. For example, Chowdhury et al. [26] examined how MUD can moderate the communication of devices in healthcare contexts, thus reducing the probability of unauthorized manipulation. Anomaly detection techniques were also combined with MUD by Quintero et al. [27] to increase the accuracy of detection of unauthorized behaviors in IoT networks. Also, Ramakrishnan et al. [28] proposed a novel extension of the MUD concept to include blockchain technology to increase the security and data integrity of IoT-based healthcare systems. These studies demonstrate the functionality of MUD in the context of healthcare security. However, as the cyber threats are increasing in complexity, there is a growing need for new and smarter security frameworks. Gupta et al. [29] examined the role of AI-based Intrusion Detection Systems (IDS) in healthcare IoT and illustrated how advanced AI models can enhance the real-time identification of threats. Therefore, this research seeks to develop a secure and robust architecture that can be readily implemented in future healthcare applications to secure data and networks.

3.1 Existing Solutions and Limitations

To address the risks in IoT environments the IETF introduced the Manufacturer Usage Description (MUD) framework to secure by restricting device communications to predefined, expected patterns. While MUD does effectively limit unauthorized access, it can't detect emerging threats that aren't part of previously detected behaviors because it is static. On the other hand, traditional Intrusion Detection Systems (IDS) use machine learning models to detect anomalies dynamically in network traffic. But these models incur high false positive rates in IoT ecosystems because of the complex, diverse communication patterns of connected devices.

3.2 Research Gap

Although MUD provides a step by step approach to securing IoT devices, this rigidity makes it ineffective in situations of environmental complexity where device behaviour is constantlychanging. On the other hand, ML based intrusion detection systems although able to detect new threats, have a tendency to fail to distinguish between normal and abnormal deviations in resource constrained IoT networks. Nonetheless, there is a growing need for adaptive security solutions, yet there is limited research on combining MUD profiles with machine learning for improved security of IoT devices in healthcare settings. This paper fills this gap by proposing a hybrid model that integrates MUD profiles with machine learning models to detect anomalies in real time.

Therefore, this paper aims at proposing a hybrid model that combines MUD and ML to detect anomalies in healthcare IoT environments.

The remainder of this paper is organized as follows: section two presents the related work. In section three, the proposed model is explained in detail. This paper presents the implementation of the model in a healthcare IoT environment in section four. In section five, the results of the detection model are discussed, and in section six, the conclusions of the paper are presented. In this paper, a hybrid model that integrates MUD and ML to detect anomalies in healthcare IoT environments is proposed. The remainder of this paper is organized as follows: section two presents the related work. In section three, the proposed model is explained in detail. This paper presents the implementation of the model in a healthcare IoT environment in section four. In section five, the results of the detection model are discussed, and in section six, the conclusions of the paper are presented.

This research is aimed at integrating MUD profiles with enhanced machine learning algorithms in order to design a new Intrusion Detection

System (IDS) for IoT-enabled healthcare environments. The authors believe that utilizing MUD's defined behavioral constraints in conjunction with the dynamic detection capabilities of machine learning can improve the accuracy of anomaly detection while minimizing false positives.

The proposed security framework consists of a two-layered defense mechanism: The first layer of the framework consists of using MUD policies to enforce restrictions on the expected device communication behaviors and the second layer of the framework consists of machine learning models that analyze the deviations and perform the detection tasks. The ultimate objective of this research is to design a adaptive security framework for secure communication of sensitive medical data and functioning of IoT enabled healthcare systems. Also, the proposed system is able to evolve with new cyber threats and provides a scalable and real-time security solution for smart healthcare environments.

4 Comparison with State-of-the-Art Methods

Several approaches have been suggested to improve the security of IoT devices, including the use of MUD profiles and machine learning algorithms. However, existing approaches have their limitations when applied to more complicated environments, such as healthcare IoT. This section compares the state-of-the-art security techniques, and the following table illustrates how our proposed model contributes to addressing the identified challenges. The table clearly shows that our proposed model, which integrates MUD and ML, effectively addresses all of the challenges identified in the framework by the IMB. Additionally, our model ensures interoperability among diverse IoT devices and applies a unified framework for securing both new and existing devices within the healthcare environment. This approach enhances the overall security of the healthcare network.

4.1 MUD-Based Approaches

In their work, Heeb et al. [13] proposed the integration of MUD profiles with machine learning for better anomaly detection in IoT networks. Though their approach improves security, it is mainly aimed at typical IoT environments and does not take into account the low latency needs essential for healthcare networks.

Morgese [20] proposed MUDscope, a tool to analyze network traffic that has been rejected by MUD profiles. Although MUDscope is good at

identifying security threats, it does not have real-time anomaly detection and does not use machine learning for adaptive threat mitigation.

Our Contribution: Our model is different from these MUD-only approaches, our model synergistically combines MUD profiling with multiple machine learning algorithms like Random Forest, XGBoost, CatBoost, and MLP. This makes it particularly dynamic and timely in detecting known and new threats in healthcare IoT environments.

4.2 Machine Learning-Based Approaches

Xu et al. [14] designed an automated machine learning framework for detecting anomalies in IoT systems. Because there are no predefined behavioural constraints, the rate of false positives is higher, lowering the reliability of the system.

Alsoufi et al. [15] used deep learning models for intrusion detection systems and were able to identify complex cyber threats effectively. Nevertheless, the computational complexity of deep learning models renders them unsuitable for deployment on resource-limited IoT healthcare devices.

Our Contribution: Our method minimizes false positives by using MUD profiling with machine learning models to build a baseline of normal device behavior. The method is more accurate in threat detection in critical healthcare applications because it follows a structured approach.

4.3 Hybrid Approaches

Yasaei et al. [16] proposed the IoT-GRAF model to improve anomaly detection by using graph learning and fusion of multi-modal data. Although the model is successful for generic IoT environments, it is not specific to healthcare and therefore cannot be easily applied to clinical settings.

Hamza et al. [23, 24] suggested an SDN-based MUD monitoring solution for smart home security applications. This model is not fully scalable to dynamic healthcare environments, which are characterized by many different types of medical devices and highly sensitive data.

Our Contribution: For healthcare IoT, we propose an approach to tailor MUD-ML integration for: a combination of static security policies with dynamic anomaly detection. The dual layered security strategy improves adaptability and guarantees real time threat detection which is critical for healthcare applications.

4.4 Summary of Contributions

Our method overcomes the limitations of existing security frameworks by:

- Combining MUD profiling with machine learning algorithms to enable adaptive, real-time detection of cyber threats.
- Reducing false positives by leveraging MUD profiles to establish a baseline for normal device communication.
- Designing a scalable and efficient security model tailored to the unique challenges of healthcare IoT networks.

A comparative evaluation of state-of-the-art approaches is presented in Table 1, summarizing the strengths, weaknesses, and key contributions of each method.

5 Research Methodology

To assess the effectiveness of MUD profiles in enhancing IoT security, we employed the ECU-IoHT dataset, which contains network traffic data from IoT devices commonly used in healthcare environments. Our research methodology consists of multiple stages, including data preprocessing, MUD profile generation, machine learning model integration, and real-time monitoring.

The process of integrating MUD profiles with the ECU-IoHT dataset and evaluating the performance of machine learning models follows a structured sequence of steps.

Figure 1 illustrates the methodology employed in this study.

5.1 Data Collection and Preprocessing

5.1.1 Dataset selection – ECU-IoHT dataset

- The ECU-IoHT dataset was chosen for its relevance in IoT-enabled healthcare applications. It contains detailed network traffic data from various medical devices.
- This dataset provides both normal and anomalous traffic, which aids in effectively training machine learning models for anomaly detection.
- **Load Data**: The dataset is imported into the working environment for preprocessing.

5.1.2 Preprocessing the data

- Encode categorical features using label encoding.

Table 1 Comparison of state-of-the-art methods with our approach

Method	Strengths	Limitations	Our Approach
Heeb et al. [13]	MUD-ML integration enhances anomaly detection	Limited to general IoT, lacks healthcare-specific optimizations	MUD-ML hybrid model tailored for healthcare IoT, enabling real-time detection
Morgese [20]	Threat analysis using MUD-based rejected traffic	No real-time detection, lacks ML integration	Incorporates real-time ML-driven anomaly detection using MUD profiles
Xu et al. [14]	Automated ML for anomaly detection	High false positives, lacks predefined behavior validation	Reduces false positives by utilizing MUD profiles to set baseline behavior
Alsoufi et al. [15]	Deep learning improves detection accuracy	Computationally expensive for resource-limited IoT devices	Optimizes lightweight ML models to integrate with MUD, ensuring efficiency
Yasaei et al. [16]	Graph learning with multi-modal fusion	General IoT focus, lacks specialization for healthcare	Healthcare-specific integration of static MUD profiling with dynamic ML detection
Hamza et al. [23, 24]	SDN-based MUD monitoring for IoT security	Smart-home oriented, lacks scalability for healthcare	Adaptive healthcare IoT security solution integrating MUD with ML for real-time learning
DeKeersmaeker et al. [25]	Profile-based firewall for smart home device interactions	Static approach, lacks adaptability for evolving threats	Combines static MUD profiling with flexible ML models for healthcare IoT security

- Normalize numerical features using MinMaxScaler.
- Split the dataset into training and testing sets.

5.2 MUD Profile Creation

MUD profiles define the expected network behavior of IoT devices, specifying parameters such as communication protocols, port numbers, and IP addresses. These profiles are stored in JSON format, making them adaptable for real-time policy enforcement.

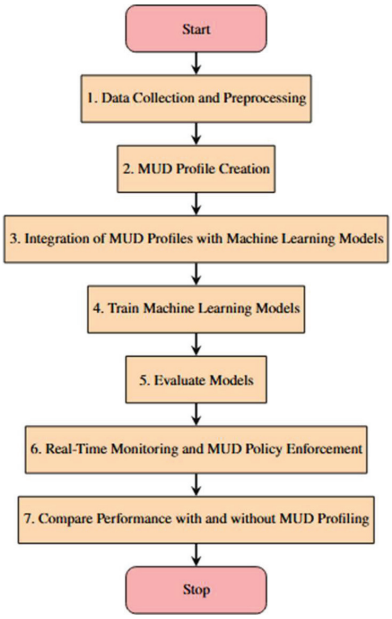

Figure 1 Process flow for integrating MUD with the ECU-IoHT dataset and evaluating ML performance.

5.2.1 Generate MUD profiles

Define MUD profiles for each device, specifying allowable communication patterns.

5.2.2 Save MUD profiles

Store MUD profiles in JSON format for real-time monitoring.

5.3 Integration of MUD profiles with machine learning models

The integration process involves real-time traffic monitoring and detecting deviations from predefined MUD profiles. Deviations are analyzed using trained machine learning models.

Figure 2 illustrates the integration of MUD profiles with Machine Learning models.

5.4 Training Machine Learning Models

To make sure that the anomalies are identified correctly, the training of various machine learning models is performed using the features that are

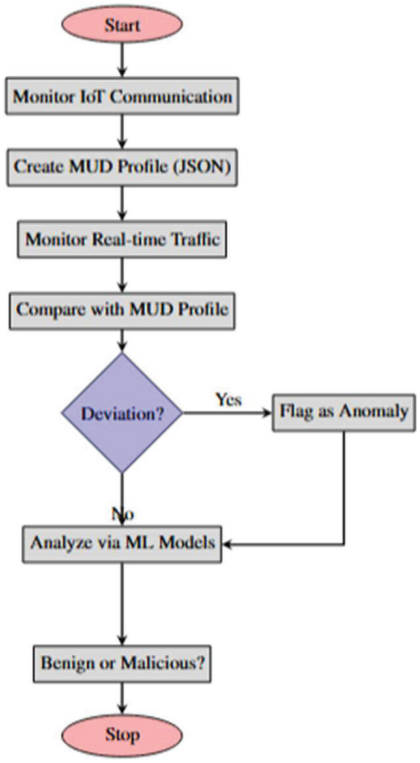

Figure 2 Flow diagram for integration of MUD profiles with ML models.

extracted from network traffic data. Each model is chosen for the specific type of attack that it can help to identify and prevent, while also minimizing the number of false positives.

- **Random Forest Classifier**: An ensemble learning model that works by building many decision trees and then combining them to reduce the prediction error.
- **CatBoost Classifier**: A gradient boosting model specifically tuned to deal with categorical features, preventing overfitting and performing very well with structured datasets.
- **XGBoost Classifier**: A powerful gradient boosting algorithm that is optimized to work with large datasets and to improve detection performance.
- **MLP Classifier**: A deep neural network based multi layer perceptron for detecting complex patterns in network traffic anomalies.

5.5 Evaluating Models

- Determine performance metrics: accuracy, recall, F1-score and precision.
- Save evaluation results for future comparison.

5.6 Real-time Monitoring and MUD Policy Enforcement

- Watch network traffic and clean it up.
- Use trained models to detect anomalies.
- Implement MUD policies to validate that the behavior is normal.

5.7 Comparison of Performance With and Without MUD Profiling

- Compare detection accuracy, false positive rates and F1 scores.
- Evaluate how MUD affects anomaly detection in IoT environments.

6 Experimental Setup

The experiment is performed using the ECU-IoHT dataset on Google Colab, a cloud based computing platform that provides necessary computing resources to train the machine learning models. This makes the model easy to deploy and also helps in incorporating MUD profiles to improve IoT security.

To achieve this, the free-tier version of Google Colab [30] is employed, which gives you a Tesla K80 GPU, 12.69GB of RAM, and around 358.27 GB of disk space. It has some essential Python libraries like pandas, scikit-learn, keras, catboost, and xgboost already installed and ready to use for data preprocessing, training and evaluating machine learning models.

The ECU-IoHT dataset is imported using pandas, which enables structured data handling and analysis. Catalognic variables are processed by LabelEncoder and numerical features are normalized by MinMaxScaler from scikit-learn to scale feature values to improve model efficiency. The computational power of Google Colab is leveraged to perform training and evaluation without having to rely on local hardware.

6.1 Real-Time MUD Policy Enforcement Mechanism

To guarantee that IoT devices converse according to set rules MUD policies are enforced in real time.

The enforcement mechanism consists of three key steps:

- **Traffic Monitoring**: Packet sniffers are used to capture live network traffic to real-time data from connected IoT devices.
- **Preprocessing**: The captured traffic data is processed using the same transformations which were used during model training to ensure consistency.
- **Anomaly Detection and Response**: Pre-trained machine learning models compare network traffic against MUD defined behaviors to detect deviations and trigger security actions, such as blocking unauthorized traffic or generating alerts.

This real-time enforcement mechanism provides rapid responses to security threats, which is especially important in healthcare settings where rapid intervention is crucial.

6.2 Dataset Selection Mechanism

The ECU-IoHT dataset is a particular collection of network traffic data from healthcare environments where IoT devices are deployed. It holds features like device addresses, port numbers, packet sizes and network security indicators that can be used to distinguish between typical and atypical traffic flows.

For model training and evaluation, an 80-20 ratio of the dataset is used to split it into training and testing sets.

6.3 Machine Learning Algorithms Selection Mechanism

To analyze network security and detect anomalies, multiple machine learning models are employed, each selected for its efficiency in handling complex patterns in IoT traffic.

- **Random Forest**: An ensemble learning model that improves classification accuracy by aggregating multiple decision trees while minimizing overfitting.
- **CatBoost**: A gradient boosting algorithm optimized for categorical data, preventing overfitting and improving model generalization.
- **XGBoost**: A high-performance boosting algorithm designed for large-scale data analysis with optimized regularization techniques.
- **MLP Classifier**: A neural network-based model that captures complex relationships in network traffic data, enhancing anomaly detection.

Table 2 Selected features of the ECU-IoHT dataset

Feature	Description
Dir	Direction of network traffic
SrcAddr	Source IP address of the device
DstAddr	Destination IP address of the device
Sport	Source port number
Dport	Destination port number
SrcBytes	Number of bytes sent from the source
DstBytes	Number of bytes sent to the destination
Temp	Temperature sensor reading
SpO2	Blood oxygen saturation level
Pulse Rate	Pulse rate of the patient
SYS	Systolic blood pressure measurement
DIA	Diastolic blood pressure measurement
Heart Rate	Heart rate measurement
Resp Rate	Respiratory rate measurement
Attack Category	Type of network attack detected
Label	Indicator of normal or malicious traffic

Each model is trained on network traffic features extracted from the dataset, ensuring precise anomaly classification.

6.4 Performance Evaluation Metrics

The effectiveness of each model is measured using standard evaluation metrics:

- **Accuracy**: Measures the overall correctness of model predictions.
- **Precision**: Evaluates how many of the detected anomalies are actual threats.
- **Recall**: Measures the model's ability to detect all relevant anomalies.
- **F1-score**: Provides a balance between precision and recall, offering a comprehensive evaluation metric.

6.5 Real-Time Traffic Monitoring and Anomaly Prediction

During real-time monitoring, the trained machine learning models classify network traffic into normal or malicious categories. This process involves:

- **Live Traffic Monitoring**: Observing network activity and analyzing real-time traffic patterns.

- **Anomaly Prediction**: Machine learning models classify network packets based on learned behavioral patterns.
- **Policy Enforcement**: MUD profiles are enforced dynamically to restrict unauthorized device communications and mitigate security risks.

6.6 Impact of MUD Profiling on Model Performance

The role of MUD profiling in network security is evaluated in two settings:

- **Without MUD Profiling**: Machine learning models are trained on raw network traffic data without enforcing MUD-defined communication rules.
- **With MUD Profiling**: The same models are trained with MUD profiles applied, establishing baseline communication patterns and reducing false positives.

A comparative analysis highlights the impact of MUD enforcement on anomaly detection, demonstrating its effectiveness in improving security while maintaining model accuracy. This experimental setup presents a comprehensive approach to securing IoT-enabled health-care networks by integrating MUD profiles with machine learning. By leveraging Google Colab's scalable computing resources, applying robust classification models, and enforcing real-time security policies, this study offers valuable insights into strengthening IoT security in real-world healthcare applications.

7 Results

The incorporation of Manufacturer Usage Description (MUD) profiles into Machine Learning (ML) models has led to significant improvements in performance across multiple evaluation metrics. The enhancements were consistently observed across various models, including Random Forest, Multi-Layer Perceptron (MLP), XGBoost, and CatBoost.

7.1 Performance Improvements with MUD Profiling

For the **Random Forest** algorithm, integrating MUD profiles increased accuracy from 0.975 to 0.989, precision from 0.966 to 0.977, recall from 0.956 to 0.968, and F1-score from 0.982 to 0.992. Similarly, in the **MLP** model, accuracy improved from 0.965 to 0.992, precision from 0.986 to 0.995, recall from 0.954 to 0.996, and F1-score from 0.967 to 0.994. These

Table 3 Performance improvement with MUD profiling (relative improvement %)

Model	Accuracy	Precision	Recall	F1-Score
Random Forest	1.43%	1.14%	1.26%	1.02%
MLP	2.80%	0.91%	4.40%	2.79%
XGBoost	1.74%	1.42%	2.06%	0.71%
CatBoost	0.51%	0.71%	1.03%	0.92%

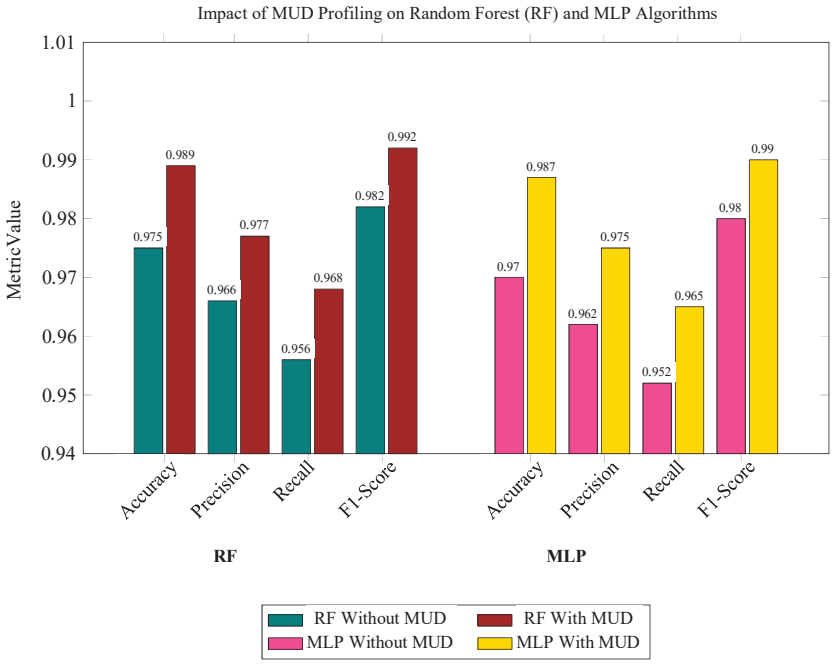

Figure 3 Evaluating impact of MUD profiling on random forest (RF) and MLP algorithms.

findings confirm that MUD profiles significantly enhance ML models' ability to distinguish between normal and anomalous network traffic.

The enhancements for Random Forest and MLP are illustrated in Figure 3.

Further analysis of the **XGBoost** and **CatBoost** models showed similar performance enhancements. The **XGBoost** model exhibited an increase in accuracy from 0.977 to 0.994, precision from 0.984 to 0.998, recall from 0.969 to 0.989, and F1-score from 0.988 to 0.995. The **CatBoost** model also benefitted from MUD profiling, with accuracy improving from 0.986 to 0.991, precision increasing from 0.985 to 0.992, recall rising from 0.972 to

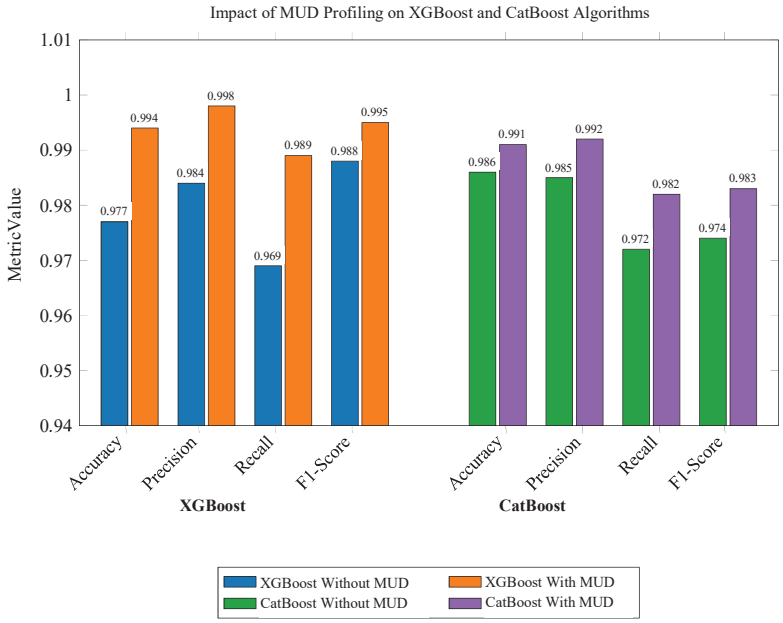

Figure 4 Evaluating impact of MUD profiling on XGBoost and CatBoost algorithms.

0.982, and F1-score improving from 0.974 to 0.983. These enhancements highlight the role of MUD profiling in improving ML models' ability to accurately detect network anomalies.

Results for XGBoost and CatBoost are represented in Figure 4.

The Table 3 below summarizes these relative performance improvements across all models.

7.2 Impact of MUD Profiling on Reducing False Positives

Incorporating MUD profiles significantly reduces false positives by establishing a baseline for normal device behavior, allowing models to more accurately detect genuine anomalies. This is particularly evident in the **MLP model**, which saw a 4.40% improvement in recall, demonstrating its enhanced ability to detect true anomalies while minimizing false alarms.

8 Conclusion and Future Work

In this study, we sought to combine Manufacturer Usage Description (MUD) profiles with machine learning algorithms to enhance anomaly detection in

IoT networks. Using the ECU-IoHT dataset, we investigated the effects of MUD profiling on different models (Random Forest, Multi-Layer Perceptron, MLP, XGBoost, and CatBoost). The results indicated that the employment of MUD profiles enhanced the accuracy, precision, recall and F1-scores of the models. Furthermore, the MLP model had a 4.40% improvement in recall, which indicates its efficiency in reducing the number of false positives. These results indicate how MUD profiles can assist in enhancing security by specifying a known good baseline of device behavior to distinguish between genuine network traffic and possible threats.

However, while MUD profiling improves security, its implementation in real life has certain difficulties. Since developing accurate MUD profiles for many IoT devices is time-consuming, and even small errors in profiling may result in misclassification or false alerts. Furthermore, real-time traffic monitoring and enforcement of MUD policies is computationally intensive and may be unfeasible in resource-limited IoT environments. Although this research was conducted on healthcare IoT, the approach can be applied to other areas, including industrial automation and smart homes that also have security issues.

In the future, there is a possibility to use reinforcement learning for the development of adaptive MUD profiles that would change their settings according to the real time traffic trends. Adaptive MUD profiles would be dynamic in nature and would therefore update themselves with respect to changing network behaviors, thus providing a better defense against the sophisticated cyber threats. This would mean that IoT security systems could learn and improve their detection capabilities automatically, with little or no human involvement.

Another interesting paradigm shift is the use of federated learning for distributed anomaly detection in large-scale IoT networks. Federated learning shares traits with ML as it trains models using data collected from different IoT devices and networks without the need to collect and store data centrally especially for sensitive applications like healthcare. Security systems designed to use a decentralized learning framework could improve detection of threats while also meeting privacy requirements.

Last but not least, deploying these adaptive models in real-life IoT applications including smart hospitals or telemedicine could give a better understanding of their practicality and performance. The real-world testing would help to reveal their computational costs and robustness in real-world conditions, so that the security mechanisms would be both effective and practical in various IoT environments.

Thus, this paper has shown that combining MUD profiling with machine learning is an effective way to improve security in IoT environments. Although challenges exist, improvements in adaptive learning and distributed security frameworks may further improve the applicability of this approach to develop more sophisticated and self-dependent IDSs for next generation IoT networks.

References

[1] Gartner's 8 Cybersecurity Predictions for 2023–2025, Gartner Report.

[2] SonicWall 2024 Mid-Year Cyber Threat Report, SonicWall.

[3] D. Kukreja, D. K. Sharma, S. K. Dhurandher, and B. V. R. Reddy, "GASER: Genetic algorithm-based secure and energy aware routing protocol for sparse mobile ad hoc networks," *Int. J. Autonomous and Adaptive Communications Systems*, pp. 230–259, 2019, doi: 10.1504/IJAIP.2019.099953.

[4] D. K. Sharma, D. Kukreja, S. Bagga, and R. Rastogi, "Gauss-sigmoid based clustering routing protocol for wireless sensor networks," *Int. J. Inf. Technol.*, vol. 13, no. 6, pp. 2569–2577, 2021, doi: 10.1007/s41870-019-00391-x.

[5] V. Soni, D. Kukreja, and D. K. Sharma, "Security vs. Flexibility: Striking a Balance in the Pandemic Era," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, 2020, doi: 10.1109/ANTS50601.2020.9342779.

[6] IETF-RFC 8520 – Manufacturer Usage Description, IETF.

[7] A. Feraudo, D. A. Popescu, P. Yadav, R. Mortier, and P. Bellavista, "Mitigating IoT Botnet DDoS Attacks through MUD and eBPF based Traffic Filtering," *arXiv*, 2023.

[8] A. Ostovar, M. Portmann, A. Arora, and K. Farkas, "Verifying and Monitoring IoT's Network Behavior Using MUD Profiles," *IEEE Xplore*, 2023.

[9] O. Garcia-Morchon, F. Kuipers, et al., "The Role of Device Identification and Manufacturer Usage Description in IoT Security," *IEEE Xplore*, 2024.

[10] N. Mazhar, R. Salleh, M. Zeeshan, and M. M. Hameed, "Role of Device Identification and Manufacturer Usage Description in IoT Security: A Survey," *IEEE Access*, vol. 9, pp. 41757–41786, 2021, doi: 10.1109/ACCESS.2021.3065123.

[11] M. Ahmed, S. Byreddy, A. Nutakki, L. F. Sikos, and P. Haskell-Dowland, "ECU-IoHT: A dataset for analyzing cyberattacks in Internet of health things," *Ad Hoc Netw.*, vol. 122, 2021, Art. no. 102621, doi: 10.1016/j.adhoc.2021.102621.

[12] K. Meena and A. Verma, "A Review of IoT Security Challenges and Solutions," *IEEE Xplore*, 2023.

[13] Z. Heeb, O. Kalinagac, W. Soussi, and G. Gu¨r, "The Impact of Manufacturer Usage Description (MUD) on IoT Security," *Zurich Open Repository and Archive (ZORA)*, 2022. doi: 10.1109/6GNet54646.2022.9830354.

[14] H. Xu, Z. Sun, Y. Cao, and H. Bilal, "A data-driven approach for intrusion and anomaly detection using automated machine learning for the Internet of Things," *Soft Comput.*, pp. 14469–14481, 2023, doi: 10.1007/s00500-023-09037-4.

[15] M. A. Alsoufi, S. Razak, M. M. Siraj, I. Nafea, F. A. Ghaleb, F. Saeed, and M. Nasser, "Anomaly-based intrusion detection systems in IoT using deep learning: A systematic literature review," *Applied Sciences*, vol. 11, 2021, doi: 10.3390/app11188383.

[16] R. Yasaei, Y. Moghaddas, and M. A. Al Faruque, "IoT-GRAF: IoT graph learning-based anomaly and intrusion detection through multi-modal data fusion," in *Proc. Design, Automation and Test in Europe (DATE)*, 2024, doi: 10.23919/DATE58400.2024.10546572.

[17] M. Imad, M. Abul Hassan, S. H. Bangash, and Naimullah, "A comparative analysis of intrusion detection in IoT network using machine learning," in *Big Data Analytics and Computational Intelligence for Cybersecurity*, Springer International Publishing, 2024, doi: 10.1007/978-3-031-05752-610.

[18] M. Baich, T. Hamim, N. Sael, and Y. Chemlal, "Machine learning for IoT-based networks intrusion detection: A comparative study," *Procedia Comput. Sci.*, vol. 215, pp. 742–751, 2022, 4th Int. Conf. Innov. Data Commun. Technol. Appl., doi: 10.1016/j.procs.2022.12.076.

[19] E. Lastdrager, C. Hesselman, J. Jansen, and M. Davids, "Protecting Home Networks From Insecure IoT Devices," in *Proc. IEEE/IFIP Netw. Oper. Manag. Symp. (NOMS)*, Budapest, Hungary, 2020.

[20] L. Morgese, "Stepping out of the MUD: Contextual Network Threat Information for IoT Devices with Manufacturer-Provided Behavioural Profiles," in *Proc. ACM Int. Workshop Comput. Sustain. Future Urban Syst. (CSFUS '22)*, 2022, pp. 7–12, doi: 10.1145/3564625.3564644.

[21] S. Wannigama, A. Sivanathan, A. Hamza, and H. H. Gharakheili, "Unveiling Behavioral Transparency of Protocols Communicated by IoT Networked Assets (Full Version)," *arXiv*, 2024.

[22] S. N. Matheu García, A. Sa´nchez-Cabrera, E. Schiavone, and A. Skarmeta, "Integrating the manufacturer usage description standard in the modelling of cyber–physical systems," *Comput. Stand. Interfaces*, 2024, Art. no. 103777, doi: 10.1016/j.csi.2023.103777.

[23] A. Hamza, D. Ranathunga, H. H. Gharakheili, M. Roughan, and V. Sivaraman, "Clear as MUD: Generating, Validating and Applying IoT Behavioral Profiles," in *Proc. ACM Workshop IoT Security and Privacy (IoT S&P '18)*, 2018, pp. 8–14, doi: 10.1145/3229565.3229566.

[24] A. Hamza, H. H. Gharakheili, T. A. Benson, and V. Sivaraman, "Detecting Volumetric Attacks on IoT Devices via SDN-Based Monitoring of MUD Activity," in *Proc. ACM Symp. SDN Res. (SOSR '19)*, New York, NY, USA, 2019, pp. 36–48, doi: 10.1145/3314148.3314352.

[25] F. De Keersmaeker, R. Sadre, and C. Pelsser, "Supervising smart home device interactions: A profile-based firewall approach," *arXiv*, 2024, arXiv:2310.03510.

[26] N. Chowdhury, S. Biswas, and M. Rahman, "IoT security in healthcare: A framework based on MUD and blockchain," *Internet of Things J.*, 2020.

[27] A. Quintero, D. Melgarejo, and L. Martinez, "Enhancing IoT security through MUD profiles and anomaly detection," *IEEE Access*, 2021.

[28] V. Ramakrishnan, M. George, and P. Kumar, "Blockchain-enabled MUD security for smart healthcare IoT systems," *J. Netw. Comput. Appl.*, 2022.

[29] A. Gupta, R. Sharma, and P. Bhardwaj, "AI-driven intrusion detection systems in healthcare IoT: A review," *J. Med. Syst.*, 2023.

[30] Google Colaboratory, Google.

Biographies

Vaishali Soni is working as a research scholar in the Department of Information Technology, Netaji Subhas University of Technology, Delhi, India. She has completed her M.E. in SOftware Systems from BITS Pilani KK Birla Goa Campus and B.Tech in Information Technology from GGSIPU Delhi. Her research focuses on the area of securing IoT environment by building novel intrusion detection and prevention systems.

Deepika Kukreja is working as an Assistant Professor in the Department of Information Technology, at Netaji Subhas University of Technology, Delhi, India. She received her M.Tech degree from YMCA and PhD from GGSIPU Delhi in Computer Science and Engineering. She has published various research papers in reputed international journals like IJCS Wiley, AIHC Springer, IJIS Springer etc. Her research areas of interest are wireless adhoc networks, Opportunistic networks, Internet of Things, Sensor Networks, Cloud Computing, Blockchain and Security systems. She has served as session chair in many conferences and is also a reviewer in various reputed journals like Transactions on Sensor Networks, Scientific Reports Springer, Wireless Personal Communications, AIHC Springer, International Journal of Mental Health and Addiction Springer etc.

Amarjit Malhotra is working as an Associate Professor in the Department of Information Technology, at Netaji Subhas University of Technology, Delhi, India. She has completed her PhD from University of Delhi. She has more than 25 years of teaching experience. Her research areas of interest are Ad hoc networks, fog computing, Machine Learning and Deep Learning biography.