Jurnal Teknik Elektro, Vol. 18, No. 1, Maret 2025: 40-45
P-ISSN 1411-870X, E-ISSN 2656-3304

CYBERSECURITY IN SMART HEALTHCARE: A MACHINE LEARNING APPROACH

Iwan Handoyo Putro
Electrical Engineering Department, Petra Christian University
Siwalankerto 121-131, Surabaya 60236, Indonesia
E-Mail: iwanhp@petra.ac.id

Abstrak – The adoption of Internet of Things (IoT) technologies in medical devices has greatly enhanced healthcare capabilities. This enables continuous patient monitoring, real-time diagnostics, and remote care. However, this connectivity also introduces significant cybersecurity threats that can compromise patient safety and system integrity. This paper presents a machine learning-based framework for detecting threats in IoT-enabled medical devices. This study utilizing the WUSTL-EHMS-2020 dataset that taking a collection of network traffic from real-world healthcare IoT systems. A comparative evaluation of multiple classifiers was conducted to assess detection effectiveness and computational efficiency. In terms of accuracy value, the Decision Tree (DT) achieves highest value of 0.97. The Random Forest (RF) model demonstrated more optimum performance across metrics with accuracy at 0.94, precision of 0.95, recall of 0.56, and F1-score of 0.70. Meanwhile, XGBoost (XGB) achieved the highest Area Under the Curve (AUC) score at 0.95, indicating strong overall classification performance. Conversely, Gaussian Naive Bayes (GNB) exhibited the weakest results, with an accuracy of 0.86, F1-score of 0.46, and the lowest AUC score of 0.73. Notably, K-Nearest Neighbors (KNN) achieved the fastest training time of just 0.001 seconds, offering a preferable option for deployment in time-sensitive environments. These results highlight the trade-offs between accuracy, speed, and robustness in machine learning-based intrusion detection systems. This study underscores the potential of intelligent threat detection models in strengthening the security of modern medical IoT infrastructures, all while balancing computational constraints.

Kata Kunci – Healthcare IoT, machine learning, cybersecurity, threat detection

I. INTRODUCTION

The rapid adoption of Internet of Things (IoT) technology in the healthcare systems has enabled the rise of smart medical ecosystem. These trends lead to development of devices that capable to perform real-time monitoring, automated diagnostics, and remote treatment. These IoT-enabled devices, including wearable health trackers, infusion pumps, and implantable sensors have significantly improved the quality of level of healthcare provision [1], [2]. However, the increased interconnectivity and reliance on networked communication expose these systems to a wide array of cybersecurity threats.

Medical IoT devices often operate under resource constraints, transmit sensitive data, and are frequently deployed in open or semi-controlled environments. This is making them an attractive target for attackers [3]. Cyber incidents involving these devices can result in unauthorized access, data leakage, tampering with medical records. Furthermore, it can disrupt of critical treatment, in which poses direct risks to patient safety [4], [5]. Conventional security approaches, such as firewalls and static signature-based intrusion detection systems, are inadequate in dealing with the dynamic and evolving nature of attacks in healthcare-focused IoT infrastructures [6].

Therefore, recent research has turned to machine learning (ML) as a promising approach for enhancing threat detection capabilities in IoT health-based systems [7]. ML-based intrusion detection systems (IDS) can learn patterns of normal and abnormal behavior from data. This allows models to identify both known and novel threats with minimal human intervention. These systems offer adaptability, scalability, and potential for real-time operation. As such, it makes them well-suited for deployment in heterogeneous and bandwidth-limited medical IoT environments [8], [9].

This study investigates the use of supervised ML techniques for detecting threats in IoT-enabled medical devices. Utilizing the WUSTL-EHMS-2020 dataset, we explore the effectiveness of multiple classification algorithms. The goal is to assess their feasibility for real-time intrusion detection under the computational and operational constraints. A typical scenario found in the medical device ecosystems.

The remainder of the paper is structured as follows: Section 2 reviews recent related work, Section 3 outlines the dataset and methodology, Section 4 presents the experimental setup and evaluation criteria, Section 5 discusses the findings and its implications, and Section 6 concludes the paper with suggestions for future research.

II. RELATED WORK

The integration of Internet of Medical Things (IoMT) devices has significantly enhanced the quality of mediacl care. However, it has also introduced substantial cybersecurity challenges. Machine learning (ML) techniques have emerged as effective tools for detecting and mitigating threats in these contexts.

Studies have explored ML-based intrusion detection systems (IDS) tailored for IoMT. For instance, a comprehensive review by Kikissagbe and Adda [10] examined various ML methods, including supervised and unsupervised approaches, highlighting their effectiveness in identifying anomalies in IoMT networks. Similarly, Alalhareth and Hong [11] proposed a hybrid ensemble model for intrusion detection, demonstrating improved performance in handling IoMT security challenges through ensemble IDS.

Anomaly detection is one of the key methods used to identify potential threats in IoMT systems. Chatterjee et al. [12] reviewed a variety of anomaly detection methods, emphasizing the importance of adapting algorithms to the specific characteristics of IoMT networks. These methods include clustering-based techniques, autoencoders, and decision trees, which are particularly useful for detecting

unusual patterns in healthcare data. Al Shahrani et al. [13] propose an optimized hashing algorithm with digital certificates to enhance the security of IoT-based healthcare systems.

While deep learning has become increasingly prominent in cybersecurity, traditional machine learning methods still play a significant role in IoMT security. For instance, to identify and distinguish attack attempts, Kumar et al. [14] proposed a hybrid deep learning model that embedded ensamble learning with their proposed One-Dimensional Convolution Long Short-Term Memory (1D-CLSTM) Neural network. Their results shows that the accuracy of the model can achieve 100% accuracy value by using WUSTL-EHMS-2020 dataset.

Several works have focused on ensuring the security and privacy of IoMT systems. ElSayed et al. [15] proposed a zero-trust architecture for healthcare IoT networks. It aims to enhance security without relying on trust between devices. This model utilizes machine learning to continuously monitor and adjust security protocols based on real-time network traffic analysis. Additionally, Al-Juboori and Jimoh [16] highlighted the vulnerabilities in medical devices, such as pacemakers. They suggested a ML-driven security mechanisms to mitigate attacks like data injection and physical tampering.

The IoMT landscape poses unique cybersecurity challenges due to the diversity of devices. Moreover, this challanges need to be addressed carefully as new threats keep emerging and exploit system weaknesses [17]. Gelenbe et al. [18] addressed the challenges of maintaining security in heterogeneous IoT-based health systems. They proposed a self-adaptive ML approach to detect and mitigate attacks across different device types. Their work emphasizes the need for fully online and collaborative learning-based AI to improve security in health systems.

III. METHODOLOGY

In this study, we employ six machine learning models: Stochastic Gradient Descent (SGD), Random Forest (RF), Decision Tree (DT), Gaussian Naive Bayes (GNB), XGBoost (XGB), and K-Nearest Neighbors (KNN). These algorithms are utilized to detect intrusions in IoT-enabled medical devices using the WUSTL-EHMS-2020 dataset.

Figure 1 shows the proposed experiment conducted in this study. Due to the limited size of the dataset, no feature selection techniques were applied, as the dataset did not contain a sufficient number of features to justify the need for dimensionality reduction.

Each model was trained and evaluated based on its ability to classify network traffic. The model performances measured using key metrics such as training score, accuracy, precision, recall, F1-score, training time, and Area Under the Curve (AUC). The goal of the methodology is to assess the effectiveness of these diverse models to accurately detect security threats while balancing computational efficiency and detection robustness.

The proposed experiment begins with the WUSTL-EHMS-2020 dataset, which contains labeled network traffic data from IoT-enabled medical devices. The first step in the process is data cleaning, where any incomplete and inconsistent entries are identified and removed. This is done to ensure the quality and integrity of the dataset. This stage includes handling missing values, correcting any formatting issues, and ensuring that the data is suitable for following analysis workflow.

A. *Proposed Method*

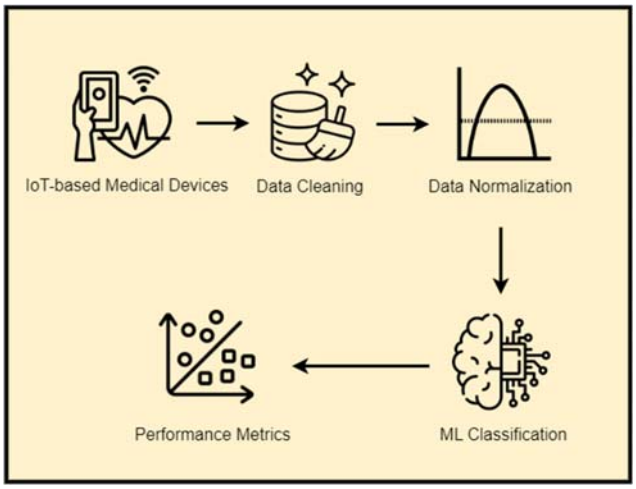

Figure 1. Proposed Experiment

Once the data is cleaned, the next critical step is data normalization. In this experiment, we use StandardScaler, a standard scaling technique to normalize the dataset. This step ensures that the features have zero mean and unit variance. It helps to standardize the range of values across different features, thus preventing any single feature from disproportionately influencing the performance of the ML models.

Following the data preprocessing stages, we proceed with the classification workflow, where six different ML models are trained and evaluated. Each model is trained on 80% of the training set and tested on the remaining 20% of the testing set. The models are assessed using key performance metrics, including accuracy, precision, recall, F1-score, and area under the curve (AUC), to evaluate their ability to correctly classify network traffic as either normal or attack traffics.

The final step involves performance evaluation, where the results from each model are compared to determine the most effective algorithm for intrusion detection in IoT-enabled medical environments.

B. *WUSTL-EHMS-2020 Dataset*

The WUSTL-EHMS-2020 dataset is a collection of network traffic data specifically designed for evaluating IDS in healthcare environments. Collected from a real-world healthcare infrastructure, the dataset contains both normal and malicious network traffic (see Figure 2). This makes it suitable for training and testing machine learning models aimed at detecting anomalies and security breaches. The dataset provides a valuable resource for evaluating how well IDS algorithms can identify threats in complex, time-sensitive environments, such as medical networks, particularly where data privacy and patient safety are important.

One of the key characteristics of the WUSTL-EHMS-2020 dataset is its diversity and real-world relevance. The data captures a wide range of activities that occur in healthcare IoT environments. This includes normal interactions between medical devices and the network, as well as potential malicious activities such as unauthorized access, denial-of-service (DoS) attacks, and data exfiltration.

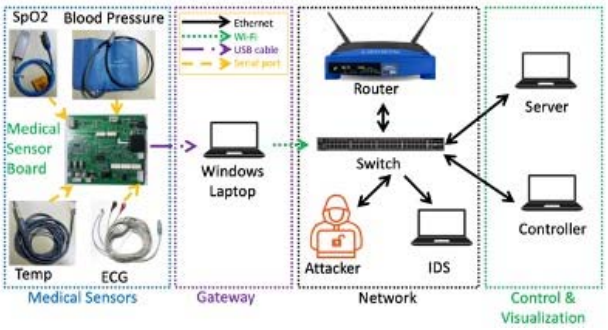

Figure 2. WUSTL EHMS Dataset Testbed [19]

This dataset is labeled with both benign and attack traffic, as can be seen in Figure 3. Label 0 for benign traffic, while label 1 is for attack attempts. This allowing seamless classfying and detection methods for the supervised training of ML models. This label enables a thorough evaluation of IDS performance. In particular in distinguishing between benign network behavior and malicious activities that could compromise the integrity of medical devices and patient data.

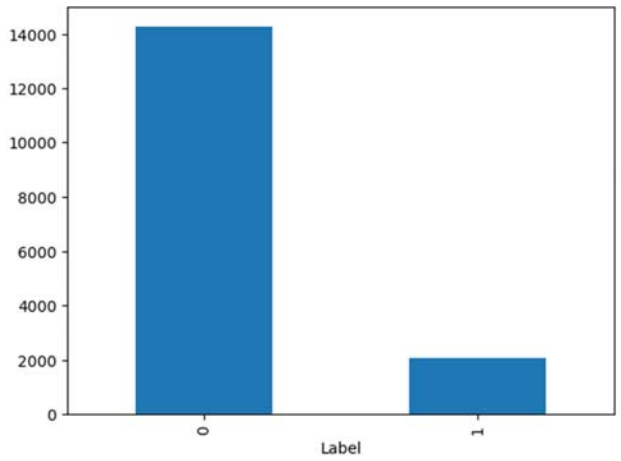

Figure 3. Comparison Between Normal and Attack Attempts

Despite its real-world origins, the WUSTL-EHMS-2020 dataset comes with some limitations. The most weaknesses of this dataset is its relatively small size compared to other benchmark datasets used in the healthcare cybersecurity domain. Tabel 1 outlines the statistical information of the dataset.

Tabel 1. Dataset Description [19]

Measurement	**Value**
Dataset size	4.4 MB
Number of normal samples	14,272 (87.5%)
Number of attack samples	2,046 (12.5%)
Total number of samples	16,318

Due to this size limitation, it may not provide the same diversity and variety of attack types or network behaviors found in larger datasets. However, it remains a valuable tool for studying the efficacy of ML-based detection methods in healthcare contexts. In particular where the trade-off between computational efficiency and detection accuracy is critical.

The dataset's focus on medical IoT systems makes it especially useful for research aimed at improving the security posture of healthcare environments. This is to ensure the safe operation of medical devices and protecting patient data from cyber threats.

IV. EXPERIMENTAL ENVIRONMENT

The experiments conducted in this study utilized the WUSTL-EHMS-2020 dataset. This dataset consists of a labeled collection of network traffic data derived from real-world healthcare IoT systems. The dataset was divided into training and testing sets with an 80:20 ratio, where 80% of the data was used for training the machine learning models and the remaining 20% was allocated for testing. The reason for this approach is to provide large enough training data so that the models can learn better.

The primary programming language employed for the implementation of the models is Python. This programming language is widely used in data analysis and having lots of machine learning libraries to work with. For data manipulation and preprocessing, Pandas was used, while NumPy facilitated numerical operations. The machine learning models were developed and evaluated using scikit-learn. This library is a comprehensive package that provides tools for model selection, training, and evaluation. For data visualization, matplotlib and seaborn were utilized to generate various plots and graphs that helped in analyzing and interpreting the results.

The experiments were run on a high-performance desktop system equipped with an Intel Core i5 13500 processor. The system had 32 GB of DDR5 RAM. This guarantees seamless operation of large datasets and the ability to execute multiple processes simultaneously without performance degradation. Data storage and access were managed by an 1 TB NVMe drive. This device provides fast read and write speeds that helped facilitate efficient data handling.

Additionally, an NVIDIA GTX 3060 graphics card was included in the system. This GPU offers graphical acceleration for certain ML workflow. The operating system used was Windows 11. It provides a stable and compatible environment for running the necessary software and libraries. This robust experimental setup ensured the models could be trained and evaluated efficiently, providing accurate and reliable performance metrics for ML models comparison.

V. RESULTS AND DISCUSSION

The results from the evaluation of several machine learning models in the context of intrusion detection systems (IDS) for IoT-enabled medical devices provide valuable insights into their performance characteristics. Table 2 provides comparison of performance matrics among ML classifiers.

Among the models tested, the DT stands out with the highest accuracy percentage as 0.97. The DT model also records recall value of 0.89. This indicates its ability to identify a large proportion of true positives cases. This functionality is essential in threat detection scenarios where missing attacks can cause severe damages.

However, despite its strong recall, the DT model's perfect training score (1.00) suggests a potential issue of overfitting. This poor generalization happens when model learns the training data too well which including noise and outliers. As consequence, although the training score appears perfect, its performance to generalize the testing data might be decreased. In the end, this may limit its model's generalizability to unseen data.

Table 2. Comparison Results Among ML Classifiers

Classifier	Training Score	Accuracy	Precision	Recall	F1-Score
SGD	0.92	0.93	0.87	0.49	0.63
DT	1.00	0.97	0.86	0.89	0.87
RF	1.00	0.94	0.95	0.56	0.70
GNB	0.86	0.86	0.43	0.50	0.46
XGB	0.94	0.94	0.97	0.56	0.71
KNN	0.96	0.94	0.82	0.68	0.74

In contrast, the RF model, while achieving a high accuracy of 0.94 and precision of 0.95, suffers from a lower recall (0.56). This indicates that it may fail to detect a significant portion of relevant attacks to the system. In the same way, XGB algorithm, which demonstrates an accuracy of 0.94 and precision of 0.97, also exhibits a relatively low recall (0.56), meaning that it perform well in correctly identifying true negatives cases but may miss some true positives. These findings suggest that XGB and RF are suitable for applications where precision is prioritized, but they may not be ideal for contexts when a system requires to detect of every potential threat.

On the other hand, SGD model achieves 0.93 accuracy but exhibits a low recall of 0.49, highlighting its deficiency to capture many true positive instances despite overall accuracy. The F1-score of 0.63 further suggests that SGD unable to provide a balance performnace between precision and recall.

KNN model, although achieving a moderate recall of 0.68 and F1-score of 0.74, giving potential in terms of computational efficiency. It has the fastest training time of just 0.001 seconds (see Table 3), making it highly suitable for applications that demand a real-time and low-latency applications.

However, its moderate performance in terms of recall and precision implies that it might miss a significant amount of attacks. This limitation might be critical in environments, such as medical device security.

Table 3. Training Score Comparison for All ML Models

Classifier	Training Score
SGD	0.059
DT	0.241
RF	4.338
GNB	0.011
XGB	9.542
KNN	0.001

Table 3 outlines the training score recorded for all ML classifiers. In terms of computational efficiency, KNN and GNB are the fastest among ot her ML algorithm used in this study. The KNN being especially outstanding for its low training time. GNB model, despite its low computational cost, performs poorly across all metrics, with an accuracy of 0.86, precision of 0.43, and F1-score of 0.46, making it unsuitable for use in this healthcare context.

The longer training times is recorded for XGB (9.542 seconds) and RF (4.338 seconds). This is indicating a disadvantage in healthcare domain where time is a sensitive constraint. Although their overall performance in terms of accuracy and precision may justify their application in less time-critical setting.

The comparative evaluation of these models reveals significant trade-offs between accuracy, recall, precision, and computational efficiency. All of which are important aspects when selecting a ML-based IDS in IoT-enabled medical devices.

The DT model, with its high recall value, is an excellent candidate for scenarios where the primary goal is to maximize the detection of threats, even at the expense of precision. This characteristic is particularly important in healthcare systems where undetected security threats could have severe consequences. However, its high training score and potential overfitting suggest that its performance may degrade when exposed to new, unseen data, which need for urgent and careful consideration of model regularization techniques to avoid overfitting.

On the other hand, the RF model, which provides an optimum performance in between accuracy and precision, might be more suitable for environments where the cost of false positives is higher than that of false negatives. The relatively lower recall could be mitigated by implementing an ensemble approach or integrating it with other models to increase sensitivity.

The XGB offers a powerful option for security systems with its exceptional precision and moderate recall. This is particularly relevant to a scenario where the cost of false positives is particularly high. In other words, the aim is to detect of rather well-known type of attacks rather than capturing all possible threats.

Nonetheless, its longer training time suggests that it may not be the best option for real-time intrusion detection in critical systems, such as health care domain. For environments where training time is a critical constraint, K-NN appears as a prospective alternative. In spite of its average recall and precision value, its ability to train data almost without delay (0.001 seconds) makes it an attractive choice for time-sensitive applications. Altough it could miss certain attacks that might otherwise be detected by more robust models like DT or RF.

Another important consideration is the computational cost associated with each model. While KNN and GNB provide the benefit of low training times, the trade-off is clear in terms of model performances, with GNB particularly under-performing in all of the evaluation metrics.

In scenarios with system having fewer limitations on computational resources, XGB and RF models still provide excellent performance, albeit at a higher computational cost. The longer training times of these models must be weighed against their higher accuracy and precision, which might be acceptable in environments where processing time is not demanding.

However, in real-time systems, where immediate action is needed, KNN provides an optimal balance between speed and reasonable detection capabilities. While K-NN may not record the optimum performance across all evaluation metrics, this model can be selected when dealing with rapid detection is essential. This can be useful as first tier of IDS system where fast respon is prefered than the careful attacks detection.

Figure 3 shows the ROC AUC curve from XGB classifier. This model achieves an impressive AUC score of 0.95, which indicates its outstanding ability to correctly classify both the positive and negative cases in IoT-enabled medical devices. This excellent performance can be attributed to XGBoost's use of gradient boosting, which sequentially refines weak learners to builds a robust and high-performance model. The

model's ability to handle complex relationships in the data and its resilience to overfitting contribute to its superior performance, particularly in the context of high-dimensional datasets like those found in the intrusion detection tasks.

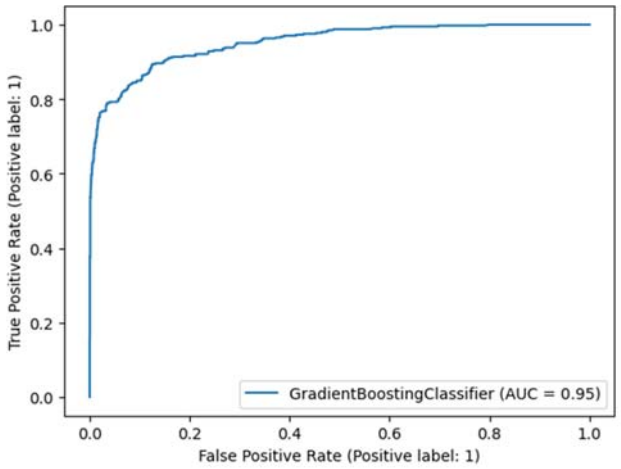

Figure 3. ROC AUC XGB Model

The high AUC score also highlights the model's versatility in dealing with imbalanced datasets. This is a common challenge in IDS in which dataset mimics the situation in network environment. In the real-world situation, the number of attack attempts is significantly lower than the normal traffic. XGB's capacity to assign higher importance to misclassified samples allows it to effectively focus on detecting minority class instances. This capability is often critical in security applications. This makes it particularly valuable in real-world IoT security scenarios where detecting rare but critical anomalies, such as cyber-attacks, is essential. In short, the high AUC score of XGB demonstrates its suitability for security applications in IoT systems, where both detection accuracy and the ability to distinguish between subtle differences in data are essential.

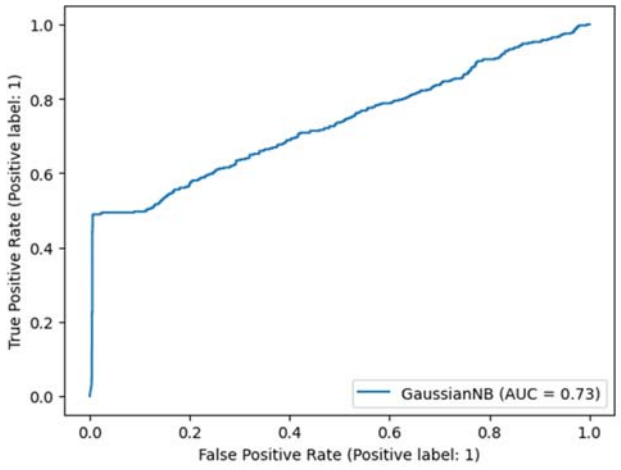

Figure 4. ROC AUC GNB Model

In contrast, GNB model recorded a considerably lower AUC score of 0.73, as it shown in Figure 4. This indicates its weaker performance in distinguishing between the positive and negative classes. This figure suggests that GNB unable to effectively identify relevant threats in the dataset. This may lead to a higher probability of misclassifications. The lower AUC also indicates that the model may have difficulty in detecting anomalies. This is in particular in the case of complex and non-linear relationships that are common in network traffic data. GNB's assumption of feature independence and its reliance on a simple probabilistic framework may limit its ability to capture hidden patterns in the data. As consequence, this explains its limited capability to perform well in this context.

Furthermore, the lower AUC score for GNB emphasizes its limitations in handling imbalanced datasets. This is a situation where the positive class (i.e. threats or attacks) in the dataset is often underrepresented. Moreover, the model's reliance on Gaussian distributions might not be sufficient to capture the true characteristics of real-world data. This might lead to poor classification performance, especially in the detection of rare but critical security events. As a result, while GNB is computationally efficient and easy to implement, its considerably low AUC score makes it less effective than more sophisticated models like XGB.

To sum up, the choice of machine learning model for IoT-enabled medical device security depends on the specific needs and constraints of the system. DT model is preferable for applications where high recall is important. The RF and XGB stand out in scenarios where high precision is essential. Meanwhile, K-NN model is best suited for real-time, low-latency applications, despite its moderate performance in terms of recall and precision. The GNB model, given its poor overall performance, is not recommended for intrusion detection in IoMT environments.

VI. CONCLUSION

This study indicates the potential of machine learning-based models in detecting cybersecurity threats within IoT-heathcare system. In terms of accuracy, the DT model outperforms other ML algorithms utlized in this experiment. Meanwhile, the XGBoost model offers the best overall classification performance. Despite their high accuracy, the RF model come with computational trade-offs. Their high accuracy percentage but require the slowest training time.

For instance, the K-NN algorithm having the fastesth training time but as demonstrated by the faster training time of K-Nearest Neighbors. These findings highlight the need for balancing detection accuracy, computational efficiency, and robustness when implementing intrusion detection systems in healthcare IoT environments, underscoring the importance of securing medical infrastructures without compromising performance.

Additionally, the results emphasize the diverse nature of IoT medical device environments, where varying levels of threat detection and system efficiency must be considered based on specific application needs. Future work could explore the integration of hybrid models or real-time adaptation mechanisms to further enhance threat detection capabilities while addressing the computational constraints of medical IoT systems.

REFERENCES

[1] M. A. Ferrag, L. Maglaras, and A. Derhab, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," Journal of Information Security and Applications, vol. 50, p. 102419, 2020.

[2] B. Al-Shargabi and S. Abuarqoub, 'IoT-Enabled Healthcare: Benefits, Issues and Challenges', in *Proceedings of the 4th International Conference on Future Networks and Distributed Systems*, 2020, pp. 1–5.
[3] S. M. Karunarathne, N. Saxena and M. K. Khan, "Security and Privacy in IoT Smart Healthcare," in *IEEE Internet Computing*, vol. 25, no. 4, pp. 37-48, 1 July-Aug. 2021, doi: 10.1109/MIC.2021.3051675.
[4] K. A. Da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. De Albuquerque, 'Internet of Things: A survey on machine learning-based intrusion detection approaches', *Computer Networks*, vol. 151, pp. 147–157, 2019.
[5] S. Goyal, N. Sharma, B. Bhushan, A. Shankar, and M. Sagayam, 'IoT enabled technology in secured healthcare: Applications, challenges and future directions', in *Cognitive internet of medical things for smart healthcare: services and applications*, Cham: Springer International Publishing, 2020, pp. 25–48.
[6] A. Al-Garadi et al., "A survey of machine and deep learning methods for Internet of Things (IoT) security," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646–1685, 2020.
[7] A. Aldahiri, B. Alrashed, and W. Hussain, 'Trends in using IoT with machine learning in health prediction system', *Forecasting*, vol. 3, no. 1, pp. 181–206, Mar. 2021.
[8] G. Zachos, I. Essop, G. Mantas, K. Porfyrakis, J. C. Ribeiro, and J. Rodriguez, 'An anomaly-based intrusion detection system for Internet of Medical Things networks', *Electronics (Basel)*, vol. 10, no. 21, p. 2562, Oct. 2021.
[9] M. Tabassum, S. Mahmood, A. Bukhari, B. Alshemaimri, A. Daud, and F. Khalique, 'Anomaly-based threat detection in smart health using machine learning', *BMC Medical Informatics and Decision Making*, vol. 24, no. 1, 2024.
[10] B. R. Kikissagbe and M. Adda, "Machine learning-based intrusion detection methods in IoT systems: A comprehensive review," Electronics, vol. 13, no. 18, p. 3601, 2024. [Online]. Available: https://doi.org/10.3390/electronics13183601
[11] M. Alalhareth and S.-C. Hong, 'Enhancing the Internet of Medical Things (IoMT) security with meta-learning: A performance-driven approach for ensemble intrusion detection systems', *Sensors (Basel)*, vol. 24, no. 11, p. 3519, May 2024.
[12] A. Chatterjee and B. S. Ahmed, "IoT anomaly detection methods and applications: A survey," Internet of Things, vol. 13, pp. 100-116, 2022. [Online]. Available: https://doi.org/10.1016/j.iot.2021.100116
[13] A. Shahrani, A. M. Rizwan, A. Sánchez-Chero, M. Rosas-Prado, C. E. Salazar, and E. B. Awad, 'An internet of things (IoT)-based optimization to enhance security in healthcare applications', *Mathematical Problems in Engineering*, vol. 2022, no. 1, 2022.
[14] M. Kumar, S. K. Singh, and S. Kim, 'Hybrid deep learning-based cyberthreat detection and IoMT data authentication model in smart healthcare', *Future Generation Computer Systems*, vol. 166, 2025.
[15] Z. ElSayed, N. Elsayed, and S. Bay, 'A novel zero-trust machine learning green architecture for healthcare IoT cybersecurity: Review, analysis, and implementation', in *SoutheastCon 2024*, Atlanta, GA, USA, 2024, pp. 686–692.
[16] S. Al-Juboori and S. Jimoh., 'Cyber-securing medical devices using machine learning: A case study of pacemaker', *Journal of Informatics and Web Engineering*, vol. 3, no. 3, pp. 271–289, Oct. 2024.
[17] M. Elhoseny *et al.*, 'Security and privacy issues in medical internet of things: overview, countermeasures, challenges and future directions', *Sustainability*, vol. 13, no. 21, 2021.
[18] E. Gelenbe, M. Nakıp, and M. Siavvas, "DISFIDA: Distributed self-supervised federated intrusion detection algorithm with online learning for health Internet of Things and Internet of Vehicles," Internet of Things, vol. 15, p. 100-115, 2024. [Online]. Available: https://doi.org/10.1016/j.iot.2024.100115
[19] R. Jain, WUSTL EHMS 2020 Dataset for Internet of Medical Things (IoMT) Cybersecurity Research, https://www.cse.wustl.edu/~jain/ehms/index.html (accessed Jan.7, 2025).