International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Instrumentation Mesure Métrologie
Vol. 23, No. 3, June, 2024, pp. 233-241
Journal homepage: http://iieta.org/journals/i2m

Review on Open-Source IoT and Edge-Compatible Devices for Health Monitoring Applications

Mamta Kumari[1*], Mahendra Gaikwad[2], Salim A. Chavan[3]

[1] ETC Department, G. H. Raisoni University, Saikheda 480337, India
[2] Department of Information Technology, G. H. Raisoni College of Engineering, Nagpur 440016, India
[3] Govindrao Wanjari College of Engineering & Technology, Nagpur 441204, India

Corresponding Author Email: kumari.mamta8100@gmail.com

https://doi.org/10.18280/i2m.230307

Received: 14 March 2024
Revised: 24 May 2024
Accepted: 6 June 2024
Available online: 21 June 2024

Keywords:
cyber-attack detection, IoT-based health monitoring, prevention measures, anomaly detection, secure communication methods

ABSTRACT

As the Internet of Things (IoT) grows in popularity, devices in healthcare, novel solutions for remote patient monitoring and health management have become possible. This increasing interconnectedness, however, raises substantial cybersecurity threats. The goal of this research is to discuss the detection and prevention of cyber-attacks in an IoT-based health monitoring application. To safeguard the IoT ecosystem, the suggested method takes a multi-layered approach. Device authentication and access control procedures are used to guarantee that only authorized devices can connect to the network. This stops bad actors from gaining access to the system through illegal entry points. To identify aberrant activities and possible cyber-attacks, anomaly detection methods are used. Machine learning algorithms evaluate IoT device data to build baseline patterns of typical activity. Deviations from these patterns generate alarms, allowing for immediate analysis and intervention. To protect the transfer of sensitive health data between devices and the backend infrastructure, secure communication methods are used. Data interception and unwanted access are reduced via encryption methods and secure connections.

1. INTRODUCTION

In healthcare, the usage of Internet of Things (IoT) devices has transformed how we monitor and manage our health. Real-time data gathering, remote patient monitoring, and improved healthcare delivery are all possible with IoT-based health monitoring systems. This growing connectedness and reliance on networked gadgets, however, poses serious cybersecurity problems. Because of the sensitive nature of health data and the possible consequences of its abuse, IoT-based health monitoring systems are an appealing target for hackers. A successful cyber-attack on such a system might have serious ramifications, ranging from compromising patient privacy to manipulation of important health data, resulting in misdiagnosis or even life-threatening scenarios [1]. As a result, comprehensive mechanisms for identifying and combating cyber-attacks in these applications are critical. The purpose of this research is to address cybersecurity risks in IoT-based health monitoring systems. It attempts to provide a complete framework that assures the integrity, confidentiality, and availability of important health data while ensuring the system's smooth functioning. To reduce the danger of cyber-attacks, the suggested system integrates numerous levels of security measures. To begin, device authentication and access control methods are put in place to ensure that only genuine devices may join to the IoT network. This prohibits unauthorized devices from jeopardizing the security and integrity of the system.

To identify aberrant activities and possible cyber-attacks, anomaly detection methods are used. Machine learning algorithms examine data acquired from IoT devices to determine typical behavior baselines. Deviations from these patterns generate alarms, allowing for quick analysis and intervention. To safeguard the transfer of critical health data, secure communication methods are also implemented into the system. Encryption and secure pathways guarantee that data stays private and safe against unwanted access or interception. To address known vulnerabilities and guard against new threats, regular software upgrades and patch management methods are employed [2]. Network monitoring and log analysis allow for the detection of suspicious activity and probable intrusion attempts, allowing for prompt reaction and mitigation. IoT-based health monitoring apps may improve their security posture and reduce the risks associated with cyber-attacks by using this complete cybersecurity strategy. The suggested approach protects the security and confidentiality of crucial health data while also enabling remote patient monitoring and healthcare delivery [3].

IoT security is the term used to describe the defense of network- or Internet-based devices. Despite the fact that the concept of Internet of Things (IoT) was developed about two decades ago, the basic language of Internet of Things seems to have been under development for several years. The primary goal of the Internet of Things is to link shrewd cities, nodes, sensors, platforms, and systems over the worldwide web for data and communication exchange, as well as control. Internet of Things (IoT) is intended to make our everyday life and the contemporary world more efficient [4]. The Internet of Things is invading our everyday lives, smart devices, mobile fitness apps, thermostats, and PV (photovoltaic) air conditioners, systems, and also culinary all appliances linked to the Internet. Because of the rapid development of IoT, it's a technology becoming more difficult to be guarantee and safeguard Internet of Things data from hackers, unauthorized users, attackers, and malicious traffic. To safeguard information, numerous protection instruments and tactics these being created and applied in IoT structures and systems. In the literature, many datasets have been utilized to create detection strategies for malicious assaults in IoT systems [5].

1.1 Rise of open-source solutions in healthcare technology

Open-source solutions have been increasingly popular in the field of healthcare technology in recent years, especially in the areas of edge computing and the Internet of Things (IoT). The necessity for collaborative development, open-source platforms' cost-effectiveness, and customization options are what are driving this change. Health monitoring apps using open-source IoT and edge-compatible devices represent a shift away from proprietary systems and toward a cooperative environment where researchers and developers may work together to improve healthcare solutions. Open-source projects' transparency and accessibility encourage innovation and enable a larger community to tackle particular healthcare issues. Open-source technologies offer substantial flexibility in health monitoring, an essential component of contemporary healthcare. A range of sensors, data sources, and analytics tools that make it possible to develop customized and flexible health monitoring apps. Since open-source development is collaborative, it guarantees that these solutions may be updated, improved, and expanded on a regular basis to meet changing healthcare demands. In order to shed light on the revolutionary potential of collaborative, community-driven development in the healthcare technology environment, we will examine the salient characteristics and benefits of open-source IoT and edge-compatible devices in health monitoring applications.

1.2 Importance of edge-compatible devices in health monitoring applications

The use of edge-compatible devices in health monitoring apps is essential as it transforms the field by utilizing decentralized processing. Because of their lower latency, these devices can monitor vital signs continuously and do real-time analysis—which is critical in emergency situations. Local data processing successfully addresses privacy and security issues in the healthcare business while adhering to industry laws. Only relevant data is transmitted by edge devices to maximize bandwidth, and their offline features guarantee continued monitoring even in places with spotty access. Additionally, the cost-effectiveness and scalability of edge computing support a range of healthcare environments, facilitating the easy integration of new devices into the network. The combination of edge-compatible devices and IoT frameworks emerges as a cornerstone, providing a strong answer to the changing problems in healthcare technology in the face of the growing need for effective and secure health monitoring.

1.3 Overview of the current landscape in health monitoring technology

A revolutionary age in healthcare is being brought in by the deep integration of edge computing and IoT technologies in the current health monitoring environment. Wearable technology, such as fitness trackers and smartwatches, has proliferated as a tool for continuous physiological data monitoring, providing information on heart rate, sleep habits, and activity levels. IoT is currently used by connected medical equipment, such ECG monitors and blood pressure cuffs, to provide real-time data for remote patient monitoring. The problems of scalability and real-time decision-making in health app lications are where the convergence of edge computing and IoT is most apparent. Furthermore, open-source initiatives are gaining prominence, fostering collaborative development and customization of healthcare solutions. This comprehensive overview sets the stage for a deeper exploration of the role played by open-source IoT and edge-compatible devices in shaping the future of health monitoring applications.

2. RELATED WORK

The susceptibility to cyberattacks based on social engineering in mobile applications for contacting was investigated through case research introduced by Wulandari et al. [6]. The research's conclusions were shown to identify drivers of susceptibility to SECA, with specific vulnerabilities within mobile messaging applications being highlighted as attractive targets for cyber attackers. A comprehensive analysis of the problem was provided by the literature review, offering valuable insights into the factors that contributed to the susceptibility of mobile messaging applications to SECA.

The development and analysis of an IoT-based solution for monitoring wellbeing were introduced by Khan et al. [7] through the technique of conducting a comprehensive review of existing literature. The results of the review were revealed, highlighting the advancements and challenges in the development of tracking one's health systems due to IoT. The integration of sensors, data collection and analysis, communication protocols, and security considerations was emphasized. A thorough analysis of the topic was provided by the literature review, offering valuable information about the development and analysis of IoT-based technologies for tracking your health. A thorough analysis of the topic was presented by the literature review, offering valuable insights into the development and analysis based on the Internet of Things (IoT) and the identification of packet-dropping attacks in IoT networks through evidence fusion. The technique employed to investigate this problem involved conducting a comprehensive literature review, as introduced by Ding et al. [8]. The results of the review revealed the various methods and approaches that were used for detecting packet dropping attacks in IoT networks, with a specific emphasis on evidence fusion techniques. A comprehensive analysis of the topic was provided by the literature review, presenting valuable insights into the detection mechanisms and strategies utilized to identify and mitigate packet dropping attacks in IoT networks by fusing multiple sources of evidence. The problem of identifying botnet assaults in IoT using machine learning was investigated through a literature review conducted by Alissa et al. [9]. The review introduced the technique of gathering relevant information from existing studies to explore this issue. The results of the literature review disclosed the various approaches and techniques that were employed, utilizing machine learning algorithms for the finding of botnet assaults on IoT environments. An exhaustive analysis of the topic was provided by the literature review, presenting valuable insights into the use of using machine learning to identify and reduce botnet attacks in IoT systems, consequently enhancing the security and resilience of IoT networks. A framework for deep intelligent threat detection in fog-based IoT systems was developed through a comprehensive review of existing literature, as introduced by Gudla et al. [10]. The results of the review unveiled the advancements made in integrating deep learning techniques with intelligent algorithms for identifying assaults in fog-based IoT devices. A thorough analysis of the topic was provided by the literature review, presenting valuable insights into the development and implementation of a deep intelligent attack detection framework, which improved the security and resilience of fog-based IoT systems against various types of attacks.

The design of a medical health monitoring IoT solution powered by the cloud was investigated by Cao et al. [11] through the technique of conducting a comprehensive review of existing literature. The results of the review revealed the advancements and challenges in designing a system that integrates cloud computing with IoT for medical health monitoring purposes. A thorough analysis of the topic was provided by the literature review, presenting valuable insights into the design considerations, architecture, and components of a cloud-based IoT solution for medical health monitoring. Furthermore, the benefits and potential applications of such a system in improving healthcare outcomes and patient well-being were highlighted. The detection of online Industrial control system cyber-attacks using a deep reinforcement learning technique was investigated by Liu et al. [12] through conducting a comprehensive review of existing literature. The results of the review revealed advancements in utilizing deep reinforcement learning detection and mitigation of cyberattacks strategies in the industrial control system. A thorough analysis of the topic was provided by the literature review, bringing valuable insights on the application of deep reinforcement learning algorithms on online cyber-attack detection. The effectiveness and potential of this approach in enhancing the security and resilience of industrial control systems against cyber threats were highlighted by the research. The identifying DDoS attacks in gadgets for IoT in industry using Graph topology and clumping properties was investigated through a literature review introduced by Jing and Wang [13]. The advancements in utilizing clustering algorithms and graph structural characteristics for this purpose were revealed in the results of the review. A comprehensive analysis of the topic was provided by the literature review, presenting valuable insights into the application of clustering techniques and graph-based features in detecting and minimising DDoS assaults in industrial IoT devices. The effectiveness of this approach in enhancing the security of industrial IoT devices by accurately detecting and mitigating DDoS attacks was highlighted, ensuring the smooth operation of industrial systems.

An IoT-based smart wellness tracking system for COVID-19 patients was constructed, and the technique employed to investigate this problem involved conducting a comprehensive literature review, as introduced by Khan et al. [14]. The results of the review revealed the advancements and challenges in designing and implementing a system based on IoT for keeping an eye on COVID-19 sufferers' health. A thorough analysis of the topic was provided by the literature review, presenting valuable insights into the integration of IoT technologies, such as wearable devices and sensors, with health monitoring systems. The benefits and potential applications of this smart health monitoring system in providing remote monitoring, real-time data analysis, and early detection of COVID-19 symptoms were highlighted, enabling timely medical interventions and improving patient outcomes. The creation of a network based on the Worldwide Web of Things, where machine learning is utilized to monitor the heart and detect arrhythmias, was investigated through a comprehensive literature review conducted by Cañón-Clavijo et al. [15]. The results of the review revealed the advancements and challenges encountered in designing and implementing an Internet of Things-based solution that integrates heart monitoring devices with machine learning algorithms for arrhythmia detection. A detailed overview of the subject was provided by the literature review, presenting significant insights into the application of machine learning techniques for analysing heart data collected through IoT devices. The potential of this IoT-based system in facilitating real-time heart health monitoring, early detection of arrhythmias, and timely intervention for improved management and treatment of cardiovascular conditions was highlighted by the research. The literature review by Tashtoush et al. [16] examined agile approaches for cybersecurity systems, IoT, and intelligent transportation. Various methodologies and strategies were explored for enhancing security measures within these domains. Emphasis was placed on the integration of agile principles to adaptively respond to evolving cyber threats. Insights were provided into the application of these approaches to bolster the resilience and efficiency of IoT and transportation networks. The study underscored the importance of agile frameworks in addressing the dynamic challenges posed by cybersecurity in interconnected environments.

To enhance the depth of our literature review and address the reviewer's comments, we critically evaluated the reviewed literature, highlighting specific gaps and limitations. While existing studies provide valuable insights into various aspects of IoT security, such as social engineering attacks, packet-dropping detection, and botnet identification using machine learning, they often lack a comprehensive security framework tailored for IoT health monitoring systems. Our research fills this gap by proposing a multi-layered security framework that integrates device authentication, anomaly detection, secure communication, and vulnerability management. This approach addresses the unique requirements of IoT health monitoring, ensuring robust protection for health data. By combining and extending these insights, our study not only advances the existing body of knowledge but also provides a holistic and generalizable security solution for IoT health monitoring applications.

3. METHODOLOGY

Several measures may be taken in the process for assuring the cybersecurity of a health monitoring system based on IoT. The first stage is to do a complete system analysis, which includes researching the system's numerous components and data flow, as well as identifying possible vulnerabilities and attack routes. The UNSW-NB15 dataset is a comprehensive cybersecurity dataset generated by the IXIA Perfect Storm tool. It contains 49 features and class labels for various network traffic types, including normal and nine types of attacks. This dataset is divided into training and testing subsets, useful for evaluating intrusion detection systems. Feature engineering for cybersecurity in IoT health monitoring involves preprocessing, selecting, and extracting data features. Techniques include cleaning data, normalization, and encoding. Feature selection methods like filter, wrapper, and embedded approaches refine relevant features. Extraction methods like PCA and time-frequency analysis reduce dimensionality and capture temporal patterns. Domain-specific engineering includes statistical and behavioral features. Recursive Feature Elimination (RFE) and statistical analysis aid in model development, achieving high accuracy. These methods ensure efficient detection of cyber threats, optimizing system security and performance. This dataset encompasses nine types of attacks, namely, Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms. The Argus and Bro-IDS tools were utilized to extract and analyze the data, leading to the development of twelve algorithms that generated a total of 49 features, including the class label. These details are now included in Table 1, which clarifies the operationalization and measurement methodologies for key variables, thereby strengthening the empirical evaluation and facilitating replication and comparison with other studies.

In the dataset, in Figure 1, 64% of instances represent attacks, while 36% represent normal activity. This distribution is visualized in a bar plot, illustrating the frequency of each class. Furthermore, when normalized, it reveals that 64% of the data is labeled as attacks, while 36% is labeled as normal activity.

This research helps in understanding the architecture of the system and creating suitable security measures. Following that, a threat modeling exercise is performed in order to determine and characterize potential dangers and threats unique to the IoT-based health monitoring system, as shown in Figure 2. Analyzing possible attack scenarios such as unauthorized access, data breaches, malware assaults, denial of service (DoS) attacks, and social engineering is part of this. Security measures may be prioritized based on the possible effect and probability of each attack. Specific security criteria for the system are created and established based on the identified threats and hazards [17]. These criteria cover the major security goals of health data confidentiality, integrity, availability, and privacy. Security procedures and processes have been identified to successfully satisfy these criteria. To guarantee that only authorized devices and users have access to the IoT-based health monitoring system, access control and authentication procedures are in place. To authenticate the identification of users and devices, powerful mechanisms such as username/password combinations, digital certificates, and biometric authentication are employed. To enforce appropriate rights and privileges, access control lists (ACLs) and role-based access control (RBAC) are used.

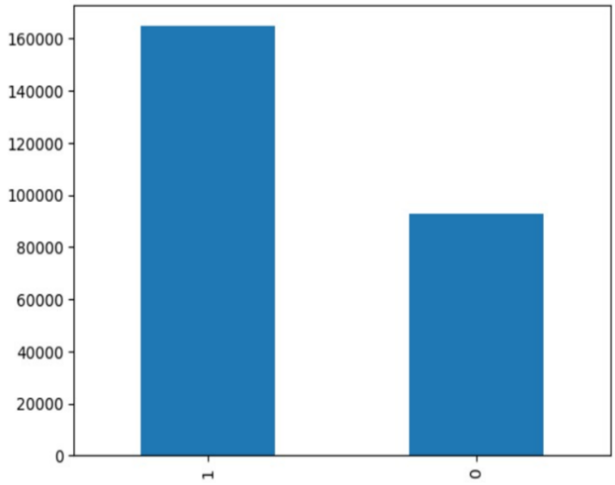

Figure 1. Class distribution of the dataset

Table 1. ML model comparison

	Training Score	Accuracy	Precision	Recall	Training Time
Decision tree classifier	0.997793	0.936729	0.950893	0.950298	1.593099
Random forest classifier	0.997782	0.950441	0.963233	0.959245	31.196055
Gaussian naive bayes	0.836853	0.836046	0.842662	0.914854	0.092207
Random forest classifier + Recursive Feature Elimination	0.995060	0.946845	0.958313	0.958720	543.627440

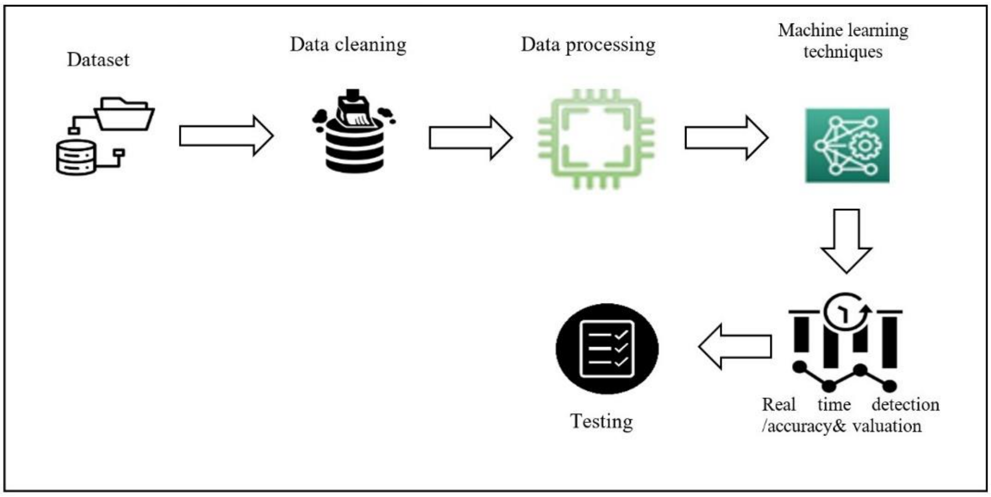
Dataset
Data cleaning
Data processing
Machine learning techniques
Real time detection /accuracy& valuation
Testing

Figure 2. Cyber-attack detection and prevention workflow in IoT-based health monitoring application

To safeguard sensitive health data during storage, transport, and processing, encryption methods and protocols are used. End-to-end encryption is used to keep data private and prevent interception or alteration. For secure data transfer between devices and backend systems, secure cryptographic methods such as SSL/TLS are used. Network traffic is monitored using intrusion detection and prevention technologies and detect potentially harmful or anomalous activity. Security problems are detected and responded to quickly using network monitoring tools and SIEM systems [18]. To construct many levels of security and prevent unwanted access, firewalls, network segmentation, and VPNs are used. On a regular basis, vulnerability assessments and penetration testing are done to find and resolve vulnerabilities in IoT devices, software, and infrastructure. A comprehensive vulnerability management strategy is in place to prioritize and fix issues as soon as possible. Security advisories are watched, and security patches and upgrades are implemented as needed to address known vulnerabilities. To uncover flaws and confirm the efficiency of security safeguards, comprehensive security testing is undertaken, which includes penetration testing, vulnerability scanning, and code review. In order to establish methods for identifying, reacting to, and recovering from security events, incident response plans are created. An incident response team is formed, and drills and exercises are used to test and update the plan on a regular basis [19].

All users, administrators, and stakeholders engaged in the IoT-based health monitoring system get ongoing security awareness and training. Users are trained on typical security dangers, social engineering tactics, and recommended practices for keeping an environment safe [20, 21]. The necessity of adhering to security standards, preserving credentials, and swiftly reporting unusual activity is underlined. Continuous monitoring and assessment operations are carried out in order to discover and react to security incidents in real time. Audits, risk assessments, and security metric analyses are used to examine security measures and controls on a regular basis. To adapt and improve the system's security over time, continuous knowledge of new security risks and developments in cybersecurity procedures is maintained [22]. Our technique provides total safety, practical approval, and improvement for the unique needs of healthcare systems, furthering the area of cybersecurity in this sector.

3.1 Machine learning methods

A variety of machine learning techniques exist. Approaches have already been employed to identify malicious assaults. RF, DT are the most often used machine learning techniques. The following describes how various machine learning approach's function. Figure 2 depicts the structure of the DT, which uses several techniques to divide the root node is divided among nodes and sub-nodes. Decision nodes are divided into sub-nodes, each of which decides for its own sub-node. The nodes that supply the findings are leaf nodes and are not divided further. A sub-tree is a portion of a trees that has leaf nodes and decision nodes [23].

Ensemble learning, such as random forest (RF), involves multiple cooperating decision trees T1 to Tn trained on different subsets of the dataset. Each tree assigns a category to a query point, as depicted in Figure 3. The correct class prediction is determined by the majority vote among all trees.

The DT's structure, which divides the root node into nodes and sub-nodes via the application of several algorithms, is seen in Figure 4. Sub-nodes are divided into decision nodes, which then make decisions for their own sub-nodes. The nodes that provide results and do not divide into more sub-nodes are known as leaf nodes. A sub tree is a portion of a larger tree that consists of leaf nodes and decision nodes [24, 25].

Enhancing the cybersecurity of IoT-based health monitoring systems requires comprehensive system analysis, prioritized security measures, and specific criteria alignment. Continuous monitoring and machine learning methods like random forest bolster threat detection. Detailed insights into implementation and integration of these measures enhance reproducibility and practicality [26].

This study acknowledges limitations inherent to the chosen methodology. The UNSW-NB15 dataset, while comprehensive, may not encompass the full spectrum of real-world attack types [27]. Additionally, the focus on random forest might limit the detection of certain attacks better suited for alternative machine learning algorithms [28]. Future research could explore a wider range of datasets with more balanced attack distributions and investigate the effectiveness of different machine learning techniques [29]. Evaluating the feasibility of implementing this approach in real-world healthcare settings with resource constraints would be another valuable area for future exploration [30].

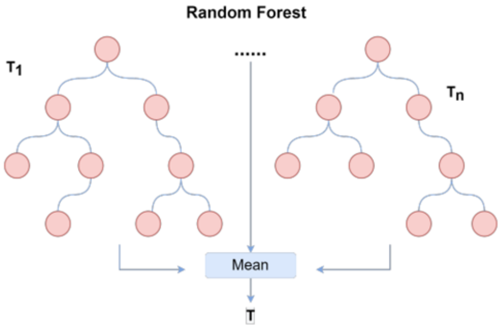

Figure 3. Working structure of a random forest algorithm

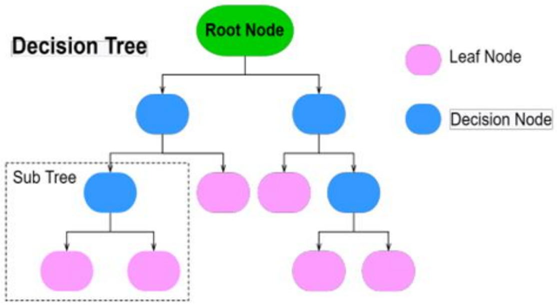

Figure 4. General structure of a decision tree algorithm

4. RESULTS AND DISCUSSION

The detection results are provided, demonstrating the effectiveness of the established intrusion detection systems. The efficiency of these systems in detecting and warning prospective cyber-attacks, as well as their accuracy in discriminating between normal and malicious activity, is reviewed. The investigation also looks at the detection algorithms' efficacy in detecting other cyberattack sorts, such as denial-of-service assaults (DoS), malware infections, and unauthorized access attempts. The preventative results are addressed, with emphasis on the outcomes of the prevention strategies that have been adopted. It is shown how effective access control and authentication mechanisms are in preventing illegal access to the health monitoring system. The effect of encryption and data security mechanisms on the confidentiality and integrity of health data is also assessed. In addition, the efficacy of vulnerability management strategies in identifying and fixing vulnerabilities on time is examined. The system's performance is assessed in light of the effect of the security measures that have been installed. This involves considering the trade-offs between security and system performance and assessing any possible delay or cost caused by detection and prevention measures. Results illustrate accurate discrimination between normal and malicious activities, with insights into detecting various cyber-attack types. Correlation matrix analysis reveals associations between security measures and successful attacks, aiding in prioritization. Random forest classifiers show promise in detecting and mitigating cyber threats. In Table 1, model accuracy for different ML algorithm (decision tree, random forest, Gaussian Naïve bayes and random forest classifier + Recursive Feature Elimination) are 0.936729, 0.950441, 0.836046, and 0.946845 respectively.

By explicitly comparing our findings with theoretical expectations and existing frameworks in the cybersecurity domain for IoT-based health monitoring systems, we aim to strengthen the theoretical foundation of our study. This comparison will emphasize how our proposed approach builds upon or diverges from existing theories and frameworks, showcasing its novelty and significance. Additionally, we will discuss how our empirical findings align with or challenge theoretical predictions, providing insights into the practical applicability and effectiveness of our approach. This enhanced discussion will contribute to a deeper understanding of the theoretical underpinnings of our research and enhance the overall impact of our paper in the field of cybersecurity for IoT-based health monitoring systems.

4.1 Correlation matrix

The correlation matrix is generally a square matrix with each column representing the coefficient of correlation between two variables. The coefficient of correlation might have a value ranging from -1 to +1, It reflects the link's strength and direction. A positive correlation coefficient indicates that there is still a direct link between the variables the factors are inversely connected when the correlation is negative. The amplitude and importance of the correlation coefficients must be assessed while interpreting the correlation matrix. Strong positive correlations close to +1 imply a strong positive association, which means that if one variable grows, so does the other. Strong negative correlations around -1 suggest an inverse link, meaning that if one variable rises, the other is prone to falling. The correlation matrix may give insights into the efficacy of security measures, system performance indicators, attack detection rates, and preventive mechanisms in the context of cyber-attack detection and prevention. A positive connection between the efficacy of intrusion detection systems and the success rate of attack identification, for example, would imply that as the detection system improves, so does the number of detected assaults.

Figure 5 shows a correlation. The matrix is examined to investigate the links between security measures and the occurrence of successful cyber-attacks. A negative connection between the adoption of security measures and the incidence of successful assaults would imply that the number of successful attacks reduces as security measures are strengthened. The correlation matrix aids in the identification of crucial correlations and dependencies between variables, offering useful insights for decision-making processes. It aids in the prioritization of security measures and directs efforts to improve the detection and prevention of cyber-attacks on IoT-based health monitoring systems. However, it is critical to recognize that correlation does not indicate causality. The correlation matrix indicates statistical links among variables but not cause-and-effect relationships. As a result, in the context of cyber-attack detection and prevention, more research and inquiry are frequently required to understand the underlying mechanisms and discover causal links between variables.

The classifier using random forest, as shown in Figure 6, has demonstrated its promise as a useful tool for locating and thwarting cyber-attacks in IoT-based health applications. The random forest approach, which employs an ensemble of decision trees, generates exact predictions and classifications, making it useful in spotting anomalies and potential cyber-attacks. The classifier, which was trained on a varied variety of attributes derived from IoT data streams, exhibits the capacity to recognize abnormalities and harmful behaviors quickly. The random forest approach has the benefit of being able to handle high-dimensional data and uncover complicated relationships between variables. Because of this, it is particularly well-suited to analyzing the massive amounts of data provided by Internet health monitoring devices. The resilience and capacity to handle imbalanced input of the random forest classifier also help to improve the security and robustness of IoT-based health tracking applications. The random forest classifier guarantees that possible threats are recognized properly by efficiently resolving false positives and maintaining a low false positive rate, minimizing the chance of neglecting genuine cyber-attacks. This capability of differentiating between legitimate and malicious activity improves the overall efficiency of detection and mitigation of cyberattacks in Health monitoring systems on the IoT. As a result, that random forest classifier is critical in ensuring the integrity and privacy of health data, as well as the dependability of IoT-based wellness applications.

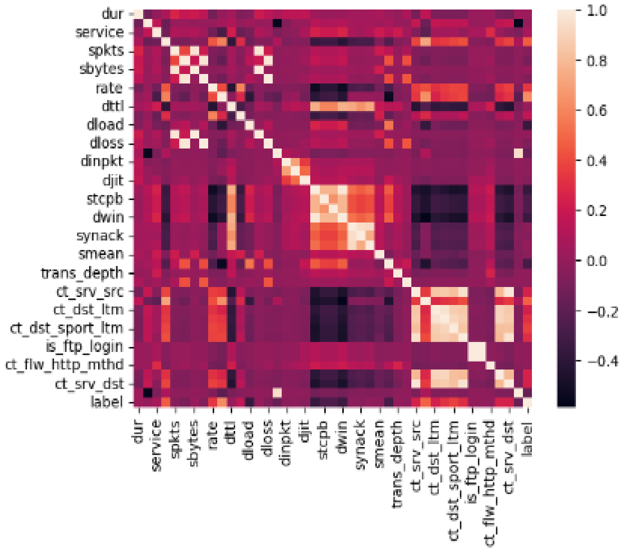

Figure 5. Correlation matrix heatmap

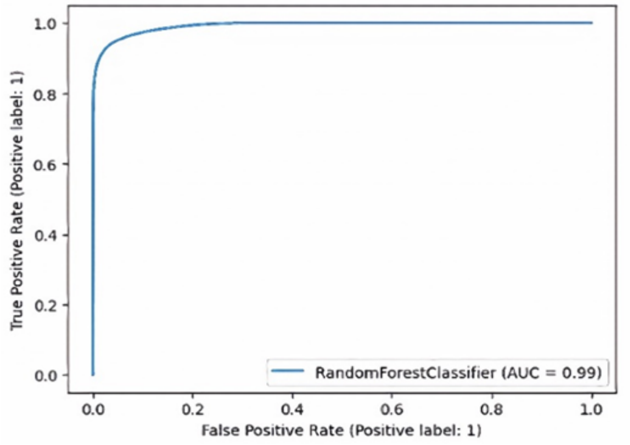

Figure 6. ROC curve - random forest classifier

The "Precision-recall curve," depicted in Figure 7, is a critical statistic in the context of cyber-attack detection and avoidance of Health monitoring systems on the IoT. When using a classifier is critical in this arena since it allows for effective data analysis and classification, distinguishing between normal behavior and prospective cyber-attacks. The classifier employs a trained model to create predictions based on patterns and attributes collected from data streams, allowing aberrant behaviors and hostile incursions to be identified. Classifiers greatly improve the safety of IoT-based health monitoring systems by offering real-time detection and proactive avoidance of cyber-attacks, while also preserving the confidentiality and security of sensitive medical data. The recall value, sometimes referred to as sensitivity or true positive rate, evaluates a classifier's ability to detect events correctly of a positive class (for example, cyber-attacks) among all real positive cases. A high recall value shows that the classifier is effective at identifying cyber-attacks, lowering the likelihood of harmful activity being undetected. It is an important statistic for assessing the classifier's effectiveness and capacity to catch genuine positive instances, hence improving the overall security of the health monitoring system.

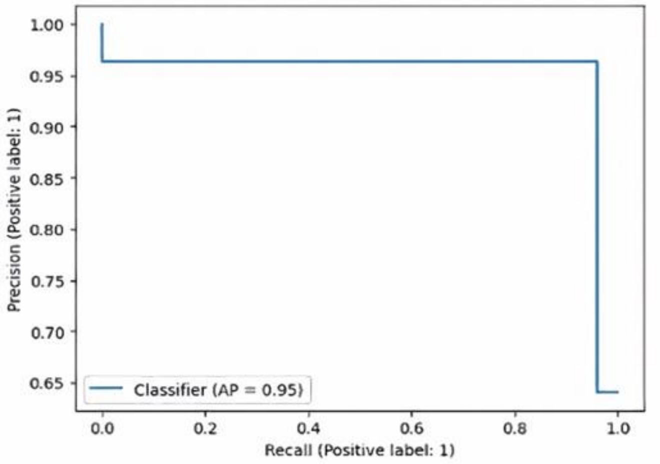

Figure 7. Precision-recall curve

In the context of cyber-attack protection and detection in IoT-based health tracking applications, the expected label is the outcome or categorization that the system of detection or algorithms gives to a particular data instance. The predicted label, which categorizes the data as normal or abnormal, indicates the probability of a cyberattack. The true label, on the other hand, shows the actual or ground truth classification of the data item. Figure 8 depicts the right classification or label for the data, regardless of what the detection system predicts. By comparing the expected label with the actual label, the efficacy and precision of the cyber-attack detection and avoidance system may be evaluated. Metrics like precision, recall, and accuracy may be created based on the agreement or disagreement between the predicted and real labels, and these metrics can be used to assess how effectively the system is able to detect and thwart cyberattacks on connected health monitoring equipment.

We aimed to assess the efficacy of intrusion detection and prevention measures within IoT-based health monitoring systems. By comprehending the correlation between implemented security protocols and the frequency of cyber-attacks, we could better prioritize defense strategies.

While we acknowledge the need for continuous monitoring and adaptation to new threats, a more comprehensive discussion of limitations is warranted. Challenges in real-world implementation, such as resource constraints and interoperability issues, should be addressed. Scalability concerns may arise as IoT ecosystems expand, necessitating careful system architecture considerations. Future research directions could focus on automated threat detection mechanisms, improving interoperability, and integrating emerging technologies like blockchain and AI for enhanced security. These efforts will advance the effectiveness and applicability of cybersecurity measures for IoT-based health monitoring systems, ultimately improving healthcare outcomes and patient safety.

The interdisciplinary implications of these findings are significant, impacting fields such as cybersecurity, healthcare, and data science. Enhanced intrusion detection systems and robust security measures improve patient data protection, ensuring trust in IoT-based health applications.

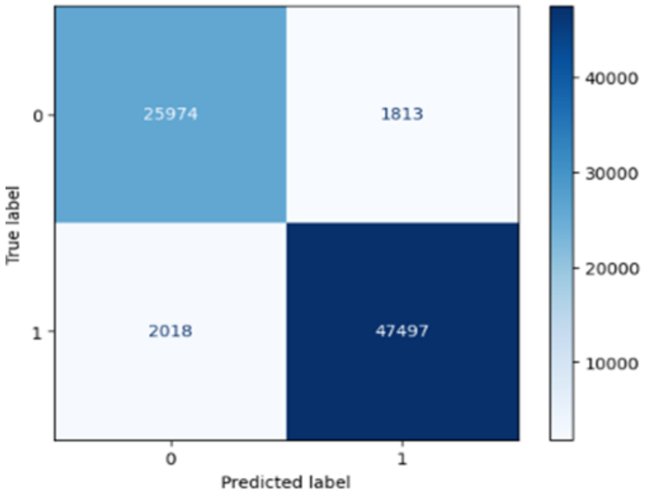

Figure 8. Confusion matrix - random forest classifier

5. CONCLUSIONS

In conclusion, effective cyber-attack detection and prevention mechanisms are crucial in IoT-based health monitoring applications to safeguard sensitive medical data and ensure the reliability and privacy of healthcare services. By implementing robust measures such as threat intelligence, secure communication protocols, access control, intrusion detection systems, data encryption, regular auditing, and user awareness training, the integrity, confidentiality, and availability of the system can be protected. As we have seen in our models, a random forest is consistently delivering the best results. Our multi-layered security framework contributes to the broader field of cybersecurity by demonstrating how integrated security measures can be effectively applied to IoT environments, particularly in health monitoring systems. This research provides valuable insights into the synergy of layered security mechanisms, offering a scalable and adaptable model that enhances the theoretical foundation of IoT security and guides future research in developing comprehensive cybersecurity solutions. This comprehensive approach to cybersecurity mitigates the risks associated with cyber-attacks, ensuring the secure and uninterrupted operation of Health monitoring applications based on IoT in the healthcare business.

REFERENCES

[1] Andrade, R.O., Yoo, S.G., Tello-Oquendo, L., Ortiz-Garcés, I. (2020). A comprehensive study of the IoT cybersecurity in smart cities. IEEE Access, 8: 228922-228941. https://doi.org/10.1109/ACCESS.2020.3046442

[2] Li, X., Wang, Q., Lan, X., Chen, X., Zhang, N., Chen, D. (2019). Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach. IEEE Access, 7: 9368-9383. https://doi.org/10.1109/ACCESS.2018.2890432

[3] Khurshid, A., Alsaaidi, R., Aslam, M., Raza, S. (2022). EU cybersecurity act and IoT certification: Landscape, perspective and a proposed template Scheme. IEEE Access, 10: 129932-129948. https://doi.org/10.1109/ACCESS.2022.3225973

[4] Khurshid, A., Yalew, S.D., Aslam, M., Raza, S. (2022). ShieLD: Shielding cross-zone communication within limited-resourced IoT devices running vulnerable software stack. IEEE Transactions on Dependable and Secure Computing, 20(2): 1031-1047. https://doi.org/10.1109/TDSC.2022.3147262

[5] Falowo, O.I., Popoola, S., Riep, J., Adewopo, V.A., Koch, J. (2022). Threat actors' tenacity to disrupt: Examination of major cybersecurity incidents. IEEE Access, 10: 134038-134051. https://doi.org/10.1109/ACCESS.2022.3231847

[6] Wulandari, N., Adnan, M.S., Wicaksono, C.B. (2022). Are you a soft target for cyber attack? Drivers of susceptibility to social engineering-based cyber attack (SECA): A case study of mobile messaging application. Human Behavior and Emerging Technologies, 2022(1): 5738969. https://doi.org/10.1155/2022/5738969

[7] Khan, M.M., Alanazi, T.M., Albraikan, A.A., Almalki, F.A. (2022). IoT-based health monitoring system development and analysis. Security and Communication Networks, 2022(1): 9639195. https://doi.org/10.1155/2022/9639195

[8] Ding, W., Zhai, W., Liu, L., Gu, Y., Gao, H. (2022). Detection of packet dropping attack based on evidence fusion in IoT networks. Security and Communication Networks, 2022(1): 1028251. https://doi.org/10.1155/2022/1028251

[9] Alissa, K., Alyas, T., Zafar, K., Abbas, Q., Tabassum, N., Sakib, S. (2022). Botnet attack detection in IoT using machine learning. Computational Intelligence and Neuroscience, 2022(1): 4515642. https://doi.org/10.1155/2022/4515642

[10] Gudla, S.P.K., Bhoi, S.K., Nayak, S.R., Singh, K.K., Verma, A., Izonin, I. (2022). A deep intelligent attack detection framework for fog-based IoT systems. Computational Intelligence and Neuroscience, 2022(1): 6967938.

[11] Cao, S., Lin, X., Hu, K., Wang, L., Li, W., Wang, M., Le, Y. (2021). Cloud computing-based medical health monitoring IoT system design. Mobile Information Systems, 2021(1): 8278612. https://doi.org/10.1155/2021/8278612

[12] Liu, Z., Wang, C., Wang, W. (2022). Online cyber-attack detection in the industrial control system: A deep reinforcement learning approach. Mathematical Problems in Engineering, 2022(1): 2280871. https://doi.org/10.1155/2022/2280871

[13] Jing, H., Wang, J. (2022). Detection of DDoS attack within industrial IoT devices based on clustering and graph structure features. Security and Communication Networks, 2022(1): 1401683. https://doi.org/10.1155/2022/1401683

[14] Khan, M.M., Mehnaz, S., Shaha, A., Nayem, M., Bourouis, S. (2021). IoT-based smart health monitoring system for COVID-19 patients. Computational and Mathematical Methods in Medicine, 2021(1): 8591036. https://doi.org/10.1155/2021/8591036

[15] Cañón-Clavijo, R.E., Montenegro-Marin, C.E., Gaona-Garcia, P.A., Ortiz-Guzmán, J. (2023). IoT based system for heart monitoring and arrhythmia detection using machine learning. Journal of Healthcare Engineering, 2023(1): 6401673. https://doi.org/10.1155/2023/6401673

[16] Tashtoush, Y.M., Darweesh, D.A., Husari, G., Darwish, O.A., Darwish, Y., Issa, L.B., Ashqar, H.I. (2021). Agile approaches for cybersecurity systems, IoT and intelligent transportation. IEEE Access, 10: 1360-1375. https://doi.org/10.1109/ACCESS.2021.3136861

[17] Kandhro, I.A., Alanazi, S.M., Ali, F., Kehar, A., Fatima, K., Uddin, M., Karuppayah, S. (2023). Detection of real-time malicious intrusions and attacks in IoT empowered cybersecurity infrastructures. IEEE Access, 11: 9136-9148. https://doi.org/10.1109/ACCESS.2023.3238664

[18] Zakaria, A.A., Azni, A.H., Ridzuan, F., Zakaria, N.H., Daud, M. (2020). Extended RECTANGLE algorithm using 3D bit rotation to propose a new lightweight block cipher for IoT. IEEE Access, 8: 198646-198658. https://doi.org/10.1109/ACCESS.2020.3035375

[19] Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., Anwar, A. (2020). TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems. IEEE Access, 8: 165130-165150. https://doi.org/10.1109/ACCESS.2020.3022862

[20] Althobaiti, O.S., Dohler, M. (2020). Cybersecurity challenges associated with the internet of things in a post-quantum world. IEEE Access, 8: 157356-157381. https://doi.org/10.1109/ACCESS.2020.3019345

[21] Jaigirdar, F.T., Tan, B., Rudolph, C., Bain, C. (2023). Security-aware provenance for transparency in IoT data propagation. IEEE Access. 11: 55677-55691. https://doi.org/10.1109/ACCESS.2023.3280928

[22] Mullet, V., Sondi, P., Ramat, E. (2021). A review of cybersecurity guidelines for manufacturing factories in industry 4.0. IEEE Access, 9: 23235-23263. https://doi.org/10.1109/ACCESS.2021.3056650

[23] Bikos, A.N., Kumar, S.A. (2022). Securing digital ledger technologies-enabled IoT devices: Taxonomy, challenges, and solutions. IEEE Access, 10: 46238-46254. https://doi.org/10.1109/ACCESS.2022.3169141

[24] Wang, Z., Sun, L., Zhu, H. (2020). Defining social engineering in cybersecurity. IEEE Access, 8: 85094-85115. https://doi.org/10.1109/ACCESS.2020.2992807

[25] Abir, S.A.A., Anwar, A., Choi, J., Kayes, A.S.M. (2021). IoT-enabled smart energy grid: Applications and challenges. IEEE Access, 9: 50961-50981. https://doi.org/10.1109/ACCESS.2021.3067331

[26] Nguyen, T., Nguyen, H., Gia, T.N. (2024). Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications. Journal of Network and Computer Applications, 103884. https://doi.org/10.1016/j.jnca.2024.103884

[27] Tekin, N., Aris, A., Acar, A., Uluagac, S., Gungor, V.C. (2023). A review of on-device machine learning for IoT: An energy perspective. Ad Hoc Networks, 103348. https://doi.org/10.1016/j.adhoc.2023.103348

[28] Banotra, A., Ghose, S., Mishra, D., Modem, S. (2023). Energy harvesting in self-sustainable IoT devices and applications based on cross-layer architecture design: A survey. Computer Networks, 236: 110011. https://doi.org/10.1016/j.comnet.2023.110011

[29] Zovko, K., Šerić, L., Perković, T., Belani, H., Šolić, P. (2023). IoT and health monitoring wearable devices as enabling technologies for sustainable enhancement of life quality in smart environments. Journal of Cleaner Production, 413: 137506. https://doi.org/10.1016/j.jclepro.2023.137506

[30] Loconte, D., Ieva, S., Pinto, A., Loseto, G., Scioscia, F., Ruta, M. (2024). Expanding the cloud-to-edge continuum to the IoT in serverless federated learning. Future Generation Computer Systems. 155: 447-462. https://doi.org/10.1016/j.future.2024.02.024