

# Securing IoT Devices in Healthcare: Endpoint Protection for Patient Monitoring Systems

**Anjan Gundaboina**

Senior DevsecOps and Cloud Architect  
USA.  
anjankumar.247@gmail.com

## Abstract:

IoT devices in healthcare have made huge strides by enhancing services, monitoring, diagnostics and treatment. Although the exponential rise of smart connected devices has brought forth effective leverage for the industry, particularly in end-point health data collection and transmission, the potential security threats synced to the development are massive. This paper aims to review the steps that can be taken in order to effectively protect IoT endpoints in the context of their use in healthcare and, more particularly, in patient monitoring systems. As a result, this paper aims to identify the possible vulnerabilities, threats, and potential attack surfaces in H-IoT applications. To achieve a robust endpoint protection mechanism, we have developed a five-fold vulnerability management plan that includes device authentication, the secure boot system, encryption of data, the adopted anomaly detection method, and the blockchain-based logging technique. We also assess the superiority of these techniques in real-time data from our simulated healthcare IoT environment and bodily-worn patients' monitors. An implication is a decreased number of instances of breach of unauthorized access and data alteration and manipulation. This research enlightens the need to apply proper security measures to the health monitoring systems in today's healthcare networks.

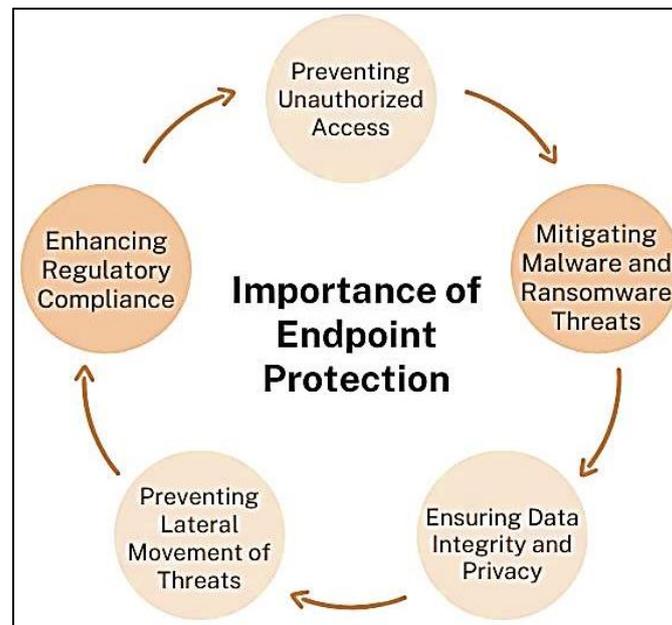
**Keywords:** IoT Security, Healthcare Systems, Endpoint Protection, Patient Monitoring, Cybersecurity, Medical Devices, Anomaly Detection.

## 1. INTRODUCTION

### *1.1. Importance of Endpoint Protection*

Endpoint protection is vital in protecting IoT-based systems, especially in the health sector, where devices always transfer secure data. It is to point out that the so-called endpoint protection makes it possible to meet risks before they can spread across the network. [1-4] The importance of endpoint protection can be elaborated in the following subtopics:

- **Preventing Unauthorized Access:** It was ascertained that endpoint protection is primarily aimed at protection from unauthorized access in IoT devices. Some IoT gadgets include patient monitors, wearables, diagnostic devices in healthcare facilities, and other information. When not well secured, these devices can be hacked or opened to unauthorized users, and different malicious actions can occur. This increases the protection of the devices in that only those who have authorized access to them will be allowed to access or interact with them in any way. This is essential for ensuring that patient records remain secure and that cybercriminals can take over none of the devices.



**Fig 1. Importance of Endpoint Protection**

- Mitigating Malware and Ransomware Threats:** IoT devices are vulnerable to various malicious programs, such as malware and ransomware attacks, that can hinder the normal use of the gadgets and render patient information vulnerable. Antivirus and firewalls, particularly intrusion detection systems, are important because they prevent such threats from penetrating deeper into a system and doing more harm. For instance, if a particular device has a virus that is trying to leak patient data or cause malfunctions within the device, adequate endpoint security will neutralize the threat so that such a device is not compromised and transmit the infection to other devices in the network. This is especially so in healthcare settings, as device failure or compromised data can be disastrous.
- Ensuring Data Integrity and Privacy:** Security and privacy of data collected by IoT devices should be maintained to the highest level, especially when dealing with health data. Endpoint protection ensures that the data collected, transmitted, and stored does not go through unauthorized changes. This is done through encryption, digital signature, and access permission. The issue of data integrity is especially pressing in the healthcare sector because even small changes in the information can result in incorrect diagnoses, treatment plans, or prescribing the wrong medication. Endpoint protection will also be useful in protecting data collected by IoT devices, whereby the data will remain unaltered, and the patients' information will remain protected.
- Preventing Lateral Movement of Threats:** An attacker will try pivoting to other network systems in a typical network environment after achieving an initial foothold. Endpoint protection can help curtail this by protecting end-user devices and preventing the spread of malware or unauthorized access. This, as a result, minimizes the chances of an attacker penetrating other devices or systems on the network by decentralizing them from each other or through techniques like network compartmentalization. This is a critical concern in healthcare facilities as an intruder who gains control over one device like the smart infusion pump can get to higher rated systems like the EHR or patient monitoring systems, resulting in far-reaching insecurity.
- Enhancing Regulatory Compliance:** Medical institutions, especially those that provide care in the United States, are governed by healthcare information privacy laws such as HIPAA. It also helps implement these regulations in organisations since it is involved in the issues of data protection, the examination of device accessibility and the establishment of safe communication lines. As a result, by providing the requisite endpoint security measures, healthcare facilities can guarantee the necessary security of their devices for the patients' reports. This is to avoid repercussions and ensure the public has confidence in the medical industry.

## 1.2. Security Threats in H-IoT

There are numerous threats to securing H-IoT as it enhances the safety of patients while improving the security of the patient's data. [5,6] The following are the critical security risks in H-IoT:

- **Unauthorized Access:** In general, unauthorized access is when an unauthorized user or a device accesses the H-IoT system. This is one of the most widespread and pernicious threats in healthcare facilities, where many patients' data is produced and transferred. An attacker may try to gain unauthorized access to a system by exploiting the credentials or compromising passwords, interfaces, devices, or protocols that form an organization's authentication process. It can violate patients' rights and privacy, alter their records, or even command medical equipment like infusion pumps and pacemakers. It is necessary to protect devices from unauthorized access with the help of authentication methods, encryption, and access rights.
- **Data Interception:** Interception is intercepting data in transit, whether between IoT devices, healthcare systems, or cloud networks that are under attack. This is especially important in healthcare facilities since it may imply communicating other people's information, including medical records, conditions, and treatments. Another risk is that attackers could employ insecure lines of communication or even employ the means Man-in-the-Middle (MitM) types of attack and gain access to the communication process of data interchange. This can result in leakage of patient information, identity theft, and changes to patient data and, therefore, require extensive use of encryption and secure communication protocols like TLS/SSL.
- **Malware Injection:** Malware injection is placing some form of malicious code into an H-IoT device or network to sabotage it, render the device or network non-functional or affect the accuracy of the information possessed by such a device or network. Various malicious activities may occur due to hacking, including communication interception loading of malware, viruses, ransomware, or Trojans that can cause various problems, including stealing data or deactivating the devices. In healthcare, this can also have disastrous effects as it can compromise patients' records, completely paralyzing the monitoring systems or even holding the records and data of the healthcare providers hostage through ransomware. To avoid malware injection, one should keep the devices and software up to date with the security patch and use real-time security scanners and anti-malware programs.
- **Device Spoofing:** Device spoofing is an attack wherein an attacker creates a fake imitation of a legal device and infiltrates the network. This can range from faking the device's identity or emulating the trusted devices to evade security measures. A case that is most fitting in the healthcare setting is a man-in-the-middle attack in which an attacker could act as an implantable heart rate monitor or an infusion pump and, therefore, siphon off confidential information from the system or even input a series of instructions into the system in the same manner as the genuine device. Device spoofing erodes the IoT network, allowing many vulnerable patient privacy and safety breaches. To prevent this risk, stricter device authentication should be adopted in the network so that only trusted devices can access a restricted domain using Public Key Infrastructure (PKI).



Fig 2. Security Threats in H-IoT

### ***1.3. Securing IoT Devices in Healthcare***

IT security in technology used in the healthcare sector is crucial for safeguarding patient privacy, safety, and data integrity. As the Internet of Things extends its footprint in the healthcare sector, it is common for wearables, smart pumps, and connective imaging systems to be used for constant tracking monitoring of patients' status. [7-10] However, these devices are insecure and prone to risks such as unauthorized access, data leakage, and malware attacks and manipulation of devices can cause severe consequences, including endangering the lives of patients, as well as legal issues with the law regarding the use of technology by healthcare facilities. The recommended steps to adopt which will enhance the security of IoT devices in healthcare below avail. Device authentication is at the more fundamental level because devices are part of the user interfaces and users are typically the first to fall for the traps laid by the hackers. Any connected IoT device should be properly identified through cryptography techniques like PKI or digital certificate to prevent the connection of unauthorized devices on the network. In addition, patient data security is also ensured by encrypting the information that is being collected. Static (data in storage) and dynamic (data in motion) should be encrypted using highly secure standards such as AES-256 and TLS 1.3, respectively, to minimize cases of interception and modification by unauthorized people. Besides, IoT devices in the healthcare processes must be protected from malware and other malign programs. Security should also be maintained through updating firmware and proper patching to close exploited loopholes. Network segmentation should also be used to ensure that the medical devices are separated from other devices in the healthcare network in order to prevent penetration of risks. Also, the IoT and smart devices' daily behavior can be monitored by anomaly detection systems based on machine learning to detect malicious activity to determine security threats at an early stage. Thus, securing IoT devices in healthcare entails typical user authentication, data encryption, and monitoring and network protection measures. These measures need to be adopted to secure the Information of the patient and the medical device and for the general safety and reliability of healthcare assets.

## **2. LITERATURE SURVEY**

### ***2.1. Prior Studies on IoT Security in the Healthcare Domain***

The application of IoT technologies in the healthcare sector has offered a number of advantages, such as monitoring and diagnosing patients without their physical having to present themselves to the doctors. Thus there have been new opportunities, but it has also brought about some of the significant cybersecurity threats. [11-14] Many studies have been conducted with the purpose of analyzing diverse methods to eliminate or overcome the threats mentioned above. For instance, Zhang et al. discussed lightweight encryption models specifically for IoT devices to input a complicated cryptographic process that can run on power-restricted healthcare sensors Zhang et al. 2019. Kumar and Lee (2021) deployed proprietary AI-based anomaly detection techniques for patient monitoring tools on another front. Their work was centered on determining how the devices behave in a rather unusual manner, which might indicate being hacked. These studies show that over time, people have recognised the risks in healthcare IoT systems, and there is an effort to protect them with newer technology.

### ***2.2. Gaps in Existing Research***

Although there are vast improvements in IoT security research that have been made today, there are still some important research gaps. Many research works focus on the network-level security components, including encryption and intrusion detection, yet provide little attention to endpoint security solutions. This has left individual devices, including wearable health trackers and connected infusion pumps, at the mercy of such direct attacks. Moreover, many suggested approaches and solutions do not consider factors such as the ability of the two platforms to interface with one another and the feasibility of the solution on a large scale. In real-world healthcare scenarios, IoT systems include a composite of devices often sourced from different vendors. This means that security solutions that are not thought through with this level of diversity in mind may be hard to implement and use, which, therefore, limits their usefulness.

### ***2.3. Comparative Analysis***

A comparison is necessary for a better understanding of the current state of affairs regarding IoT security solutions for the healthcare industry. The encryption technique was analyzed by Zhang et al. mainly to

ensure data security in its transfer or communication phase. However, the websites' IIS protocol addressed all endpoint-specific vulnerabilities but did not attempt retrospective simulation. Kumar and Lee's AI-based anomaly detection was more flexible than their proposed approach as it only partially considers the endpoints' behavior while performing the simulations that may mimic real-life usage. While doing so, however, they left the user without complete protection against malicious software at the endpoint. This lack of concrete, real-world endpoint security testing makes up the first gap to be addressed by the proposed research.

#### 2.4. Need for a Unified Framework

The reviewed literature shows that there is no coherent approach implemented to IoT security in healthcare organizations; thereby, a call for a framework is recommended. Thus, such a framework should include endpoint protection, combining hardware and software protection layers. Hardware measures can be secure boot measures and trusted platform modules, and software measures may contain behavior-based intrusion detection and automatic firmware updates. These components would create layered protection if included in the framework to address the different types of cyber threats comprehensively. Furthermore, if the framework should also be made interoperable and scalable, it would increase the usefulness of the framework in various settings, especially within the healthcare context and increase its life span.

### 3. METHODOLOGY

#### 3.1. System Architecture

The architecture of secure IoT integration in the healthcare domain includes three tiers. [15-18] The occupations are IoT Devices, Gateway (Edge Computing), and Cloud Storage.

- **IoT Devices (Wearable Sensors):** The architecture starts with IoT sensors to be worn by patients to constantly record their vital signs, including temperature, blood pressure, glucose level, and oxygen saturation. These are portable, dynamic, and intended to work in real-time environments. Their main purpose is to receive and forward health information with little delay and high availability, constituting the first point of contact with the patient.
- **Gateway (Edge Computing):** The gateway is the interface between the IoT devices and the upper-level cloud architecture. Arranged at the network periphery, typically in the healthcare facility setting, provides precordial data pre-processing, filtering, and local data anomaly surveillance. This offloads the load on the cloud system and also makes sure that the response for the critical alert is faster. It also serves as a security layer that can encrypt and control access to the data before it is transmitted to the cloud.

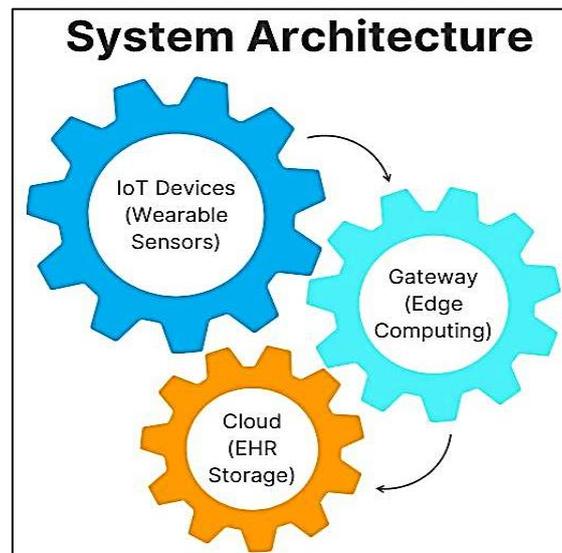


Fig 3. System Architecture

- **Cloud (EHR Storage):** The cloud layer deals with storing EHRs for long-term and complex data analysis. It allows scalability, sharing the patient's data with different sites without compromising the data's HIPAA compliance. The cloud platform also encompasses the related diagnostic services and chronological

evaluation that may help healthcare workers act according to the total data quantity and characteristics in the given time.

### 3.2. Security Layers

In the proposed architecture, more layers of security are added to protect the Healthcare IoT systems, which are aimed at addressing the various types of threats. All these layers create a holistic approach to end-to-end security.

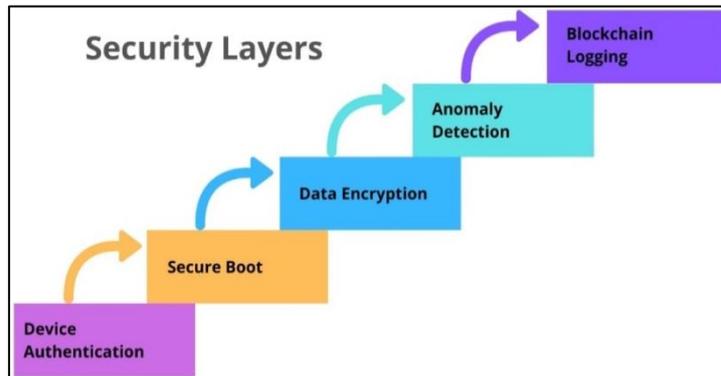


Fig 4. Security Layers

- **Device Authentication:** Device authentication is the first line of defence, and it ensures that only authorized IoT devices are allowed on the healthcare facility's network. The system uses Public Key Infrastructure (PKI) to authenticate the devices and gateways. This is done through certificates of authenticity, where the systems can recognize friendly systems and shun the vandalism under this through certificate-based authentication to ensure that only friendly system is allowed into the system.
- **Secure Boot:** Secure boot principles use Trusted Platform Modules (TPMs) that are integrated into devices in the IoT. In the startup step, the TPM examines the firmware and the rest of the software stack against a list of known good states. If there are irregularities, the boot process is stopped, which helps avoid playing out of invalid or destructive code.
- **Data Encryption:** Regarding data safety, it is safe as the data goes through encryption and other forms of protection. AES has a 256-bit key (AES-256) to encrypt medical data when stored on the device or in the cloud. The encryption standard used for data-in-transit is the Transport Layer Security (TLS) version 1.3. Any information transacted between the devices, gateways, and the cloud is protected from interception and manipulation.
- **Anomaly Detection:** Machine learning for anomaly detection is also used to identify unusual or malicious actions in real-time. Current models include Support Vector Machines (SVM) and Random Forest models that help search for patterns of the device's activity outside the observed norms. This layer improves the ability to detect threats and bring attention to any activity in real-time if a threat is indicated.
- **Blockchain Logging:** It is ensured that there is an unalterable record called block-chain. Every action and data-sharing process falls under smart contracts, making them transparent and traceable. Using blockchain characteristics, this layer ensures the non-tampering of logs, which is essential during investigations and auditing.

### 3.3. Algorithm for Anomaly Detection

The anomaly detection module has to search for patterns or trends in the sensor data stream that originate from IoT devices and alert the user in the event of any such activity. [19,20] Firstly, Preprocessing of the incoming raw sensor data stream  $S$ . This has the benefit of checking for the quality of the data in order to ensure that analysis will not be delayed due to poor-quality data. This may include activities like data cleaning, where the data is filtered and cleaned by eliminating noise, cases of missing values, normalizing the data, and there can be cases where one or many of these irrelevant data items can set back the entire process of detection. For example, noise or inconsistent signals disadvantage the analysis; hence, pre-processing facilitates the filtering of the appropriate data. After the data cleaning and pre-processing phase,

the next step is Feature Extraction from the processed data stream denoted by  $S$ . Feature engineering is essential in machine learning and anomaly detection; this involves converting given data into a more fit form for model analysis. This will include descriptive statistics, measures of central tendencies and variability, frequency distribution or temporal trend forms that could be normal or pathological. The type of features to be incorporated depends on what anomaly is being sought in the stream, whether it is outliers, drift, or a shift in the data stream. After the feature extraction step, the algorithm moves to the next step, the Prediction step, in which a trained machine learning model determines if the extracted feature is an anomaly. It could be designed using different machine learning methods, for instance, the SVM, the Random Forest or the Neural Nets. That is the case; the Alert is generated as the model has predicted that the feature set  $F$  is an anomaly. It may also alert the healthcare providers or system administrators to look into the case or circumstance further to take necessary action. It does this by adapting the basic Constant Dynamic Surveillance Scheme in real-time to form a more efficient means for identifying security threats or operational issues that require intervention quickly and efficiently.

### 3.4. Proposed Architecture

The design of the proposed system consists of three main components, namely, IDS, Blockchain-based Authentication, and Machine Learning Algorithms, in order to provide a secure and adaptive system for healthcare IoT systems.

- **Intrusion Detection System (IDS) for Anomaly Detection:** Intrusion Detection System (IDS): IDS is another important part of the overall proposed architecture; IDS is responsible for monitoring network and device activities for any anomaly behavior. Using innovative mechanisms to identify anomalous behavior, IDS always monitors data feeds originating from the IoT devices to detect signs of threats, including invasion of privacy of the devices or irregular behavior patterns among the latter. In the case of an anomaly, IDS sends out alerts, meaning that any potential danger is handled immediately. It is another layer that helps monitor and prevent or reduce the effects of an attack on the system.
- **Blockchain-based Authentication for Decentralized Identity Management:** For the purpose of solving the problems associated with effective and safe management of identities, the architecture uses distributed solutions based on the blockchain. Every IoT device, healthcare professional, and patient in this system is assigned a digital identity on the blockchain. This approach removes the dependency on a single centralized identity management system, which is vulnerable to a single point of failure, leading to improved trust and security. This makes the block blockchain's ledger open for authentication of identity transactions to be secure, and this provides a good platform for authenticating the devices and users in the health field.

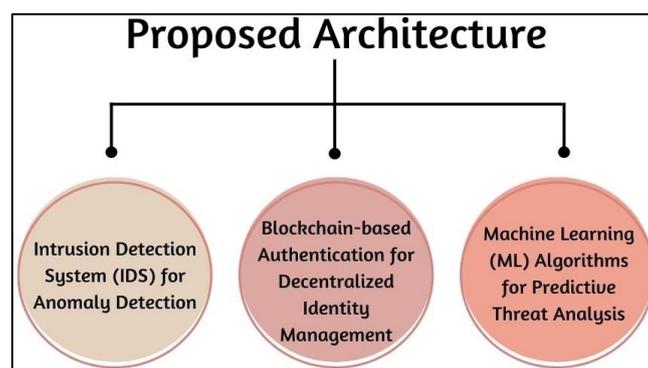


Fig 5. Proposed Architecture

- **Machine Learning (ML) Algorithms for Predictive Threat Analysis:** With the inclusion of ML algorithms into the architecture, the system can analyze future threats. These predictions can help safeguard against such threats. Supervision and anomaly detection, machine learning models are learnt to detect normal and otherwise behavior within a network. They keep learning, and even when new data are fed into them, they become more refined. Through these algorithms, the system can develop potential threats that are seen and not acted upon, making it easier to counter them before they get out of hand.

## 4. RESULTS AND DISCUSSION

### 4.1. Experimental Setup

The assessment of the proposed security framework will then involve a real-world installation of IoT devices in a simulated healthcare setup using Raspberry Pi in conjunction with biosensors to provide a physical health data feed. These IoT devices serve as the terminal points for collecting data in the healthcare environment, including heart rate, blood pressure, respiratory rate, body temperature, and blood oxygen level. These sensors ensure the patient's health is continuously monitored to identify early signs of disease or an emergency. The information that is gathered is transmitted in real-time and is later on analyzed by the various sensors. Wireshark is then used for analyzing the traffic in which the communication between the IoT devices and the network is monitored to ensure that the traffic flow is secure and any intrusive traffic is detected. TensorFlow is an open-source software toolkit for machine learning; it is employed for executing different anomaly detection algorithms on the data. These algorithms can help detect irregularities or changes in the biometric signals that may pose a security or health risk. The MIMIC-III dataset is used for training and testing the anomaly detection system, a well-known publicly available dataset. This dataset includes the patient's data stripped of identification numbers, making it suitable for training the machine learning models to detect normal and abnormal patterns in health data. Using real-world data in the experiment, the FM approach provides valuable insights into security and sensor control to detect anomalies and maintain the privacy and integrity of the protected data in healthcare.

### 4.2. Evaluation Metrics

In order to measure how well the system works in identifying anomalous activities, accuracy, and resource usage, antecedent measurement factors were captured to determine the system's efficiency in meeting the aforementioned objectives.

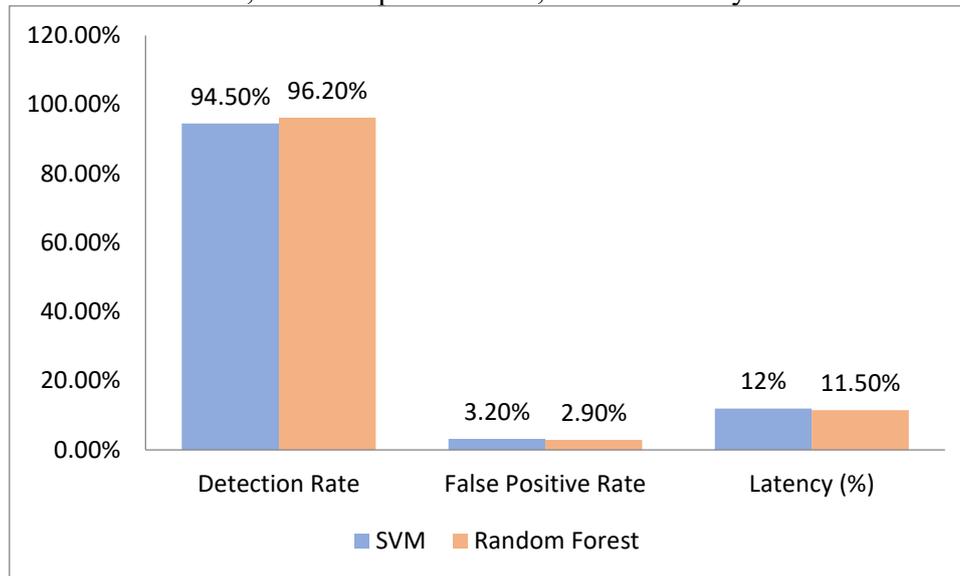
- **Detection Rate:** The detection rate is a complex performance factor that determines the capability of the system to detect any anomaly or breach in the data stream. In the context of healthcare IoT, an anomaly could be defined as either abnormal measuring values which could correspond to a pathological state or attempts of unauthorized access. A high detection rate means the system often manages to identify most of the real risks so that health providers are notified where necessary. This direction is important for patient safety and can pinpoint weak or undetected points in the system.
- **False Positive Rate:** The false positive rate means the number of normal or non-malicious behaviors the system identifies as anomalous. This can happen when the system identifies a normal and harmless variation of the patient's condition (e.g. a short-term rise or drop in heart rate) as potentially pathologic and raises alarms for it. A low FPR is better because it means there are fewer alarms that are generated that are not true, which can cause alarm fatigue among healthcare practitioners and divert the attention of the practitioners to unimportant issues. It is, therefore, important to note that both the detection accuracy and the false positive rate have to be kept very low for the system to be practical in real-life situations.
- **System Overhead:** Overhead is the cost of the hardware and software used to support the security system in delivering its services. These are the amount of CPU, memory, and bandwidth used in collecting, analyzing, and identifying the anomalous behavior of the data. In healthcare IoT systems, where many devices are required to exchange information on demand, size and latency are crucial factors. This high overhead may mean that data takes quite a long time to be processed, system responsiveness is negatively affected, and the cost of running the system is relatively high. Thus, it is necessary to evaluate whether real-time throughput can be achieved, meaning that servers, devices, or the network used in the process will become a burden. Another advantage of the proposed framework is the factor of optimising system overhead which makes the execution easy in practice.

### 4.3. Performance Results

**Table 1: Performance Results**

Method	Detection Rate	False Positive Rate	Latency (%)
SVM	94.5%	3.2%	12%
Random Forest	96.2%	2.9%	11.5%

The following are the performance measures of the two machine learning algorithms for the proposed anomaly detection methods: Support Vector Machine (SVM) and Random forest. These algorithms were selected because of their high efficiency in dealing with large data sets and the ability to find anomalies in real-time healthcare IoT context. The performance comparison of both algorithms in terms of accuracy, time complexity and number of nodes evaluated is presented in the following table. Some of the framework's measures include the detection rate, the false positive rate, and the latency.



**Fig 6. Graph representing Performance Results**

- Detection Rate:** It is the measure of the capability of a system to be accurate in identifying Outliers if they exist within the data sample. In the case of the same study, the model mentioned above has a 94.5% detection rate, which shows that the model can identify most of the anomalies with room for improvement. Random forest is also slightly better in terms of a detection rate of 96.2%, which means that the algorithm is capable of detecting a larger portion of anomalies. A higher detection rate is essential in healthcare, where the absence of such anomalies might be disastrous.
- False Positive Rate:** Whenever the system recognizes regular data as anomalous, that number is the false positive rate. In the case of SVM, the false positive rate is 3.2 %, meaning that 3.2% of normal behavior is identified as an anomaly. It can get to a point where alerts are raised when they do not need to be, which may pressure the healthcare providers or staff. On the other hand, Random Forest is marginally better regarding the false positive rate, which stands at 2.9 percent. It is always beneficial to have lower false positive rates since these alarm the healthcare providers with what is no threat at all.
- Latency:** Latency can be described as the time it takes for the system to process the data and issue an alert when an anomaly exists. SVM has a latency of 12%, so it is seen that the time to process a dataset is not too high, though real-time monitoring of the process is possible. Random Forest is a little more efficient than Naïve Bayes, with a latency of 11.5%, as it takes less time to make the same decision. Low latency of data transmission is very important if it has to do with healthcare. This is because where certain changes may likely cause a lot of harm to the patient, the system would promptly notify all the concerned parties. From the results, we can infer that SVM and the Random Forest are useful for detecting anomalies in IoT-based healthcare systems. Random Forest was slightly better than the SVM in all the assessed measures. However, both algorithms keep a good detection rate and low false alarms while keeping latencies at a minimum for real-time applications.

#### 4.4. Discussion

Therefore, from the evaluation results, it can be concluded that the proposed system architecture achieves high-quality anomaly detection and provides high efficiency in the context of healthcare IoT systems. Therefore, blockchain has a significant relevance in enhancing the security of an EMRAM with patient data. They ensure that all transactions and data sharing, as far as patient records, are recorded and sealed on the block, making it impossible for anybody to tamper with patient's records. When combined with the idea of

decentralization, where no single node controls the system's actions, the randomness of this system makes it more difficult for hackers to target any particular area and bring down the blockchain. The Random Forest algorithm and the other machine learning algorithms used for anomaly detection greatly enrich the system's learning ability to identify emerging threats in real time. These algorithms are best suited to analyze patterns emerging from the sensor data and immediately discern any variation that may indicate a security threat or medical distress from the normal pattern. Additionally, low rates of false positives in the Random Forest algorithm means that the healthcare providers are not overloaded with alerts they do not need, making the system more user-friendly and enabling healthcare professionals to tend to real threats or problems arising without distracting noise in the data.

Another important point is that the response time of the suggested system is significantly low. In the next response times, SVM and Random Forest take almost the same time to process the loads with a response time of around 115-120ms. This is important in Health care facilities since a failure to identify or act on emerging abnormalities can be fatal. Because latency is kept at a minimum, the system can quickly send feedback and alerts to enable clients to make the right decisions within the right time from the healthcare providers. Therefore, the proposed architecture meets the following requirements of high detection accuracy, very low false positives, low system overhead and low latency of the system, which makes it imperative for use in the protection of IoT devices in healthcare. In the transitions of this work, it will be possible to improve the performance of these algorithms and include other securities like encryption and access controls in future systems.

## 5. CONCLUSION

This paper presents a systematic solution to protect the endpoint in IoT-based patient monitoring systems, which are becoming more common in healthcare settings to monitor patients' health statuses in real-time. With health monitoring gadgets and other devices becoming a part of popular IoT technology, it is paramount to establish a method that can help secure health-sensitive data. The proposed system architecture follows a multilayer system, thus incorporating certain measures to prevent any point of vulnerabilities in the system. The first layer aims to ensure that only authorized devices are allowed to enter the system and communicate with the other layers through Public Key Infrastructure (PKI). The second layer concerns data communication security through AES-256 encryption of static data and TLS 1.3 to avoid making unauthorized intercepts or corrupting the health data being transmitted. Additionally, the system also incorporates real-time anomaly detection based on the signals obtained from the machine learning technique that checks the patient information regularly for any abnormality in patterns that may be existent security threats as well as possibly existing signs of any worsening in the patient's health. These strategies are planned to operate parallel to each other for the set goals: to protect patient data and keep the healthcare providers informed about the existing security threats/medical peculiarities as soon as possible.

### 5.1. Future Work

In the given proposed architecture, which focuses on the security of IoT-based patient monitoring systems, there are opportunities for further enhancement and inclusion. The future work will consider expanding the system to include more categories of H-IoT devices beyond wearables: connected medical imaging devices, infusion pumps, diagnostic equipment and others that are now also connected to the network. It will also give them a more comprehensive security model for the healthcare IoT environment. Moreover, improving machine learning is another avenue suitable for future work. The current implementation is based on algorithms like the simple and rational Support Vector Machine (SVM) random forest, and it could also be further developed with deep learning techniques like artificial neural networks and Convolutional Neural Networks (CNN). These types of advanced techniques are capable of learning from more detailed patterns in data. They could be better at identifying nuances in situations that the basic models might not. Last but not least, the connections to national health information systems are an area for improvement for future studies. If connected with broader national health network systems like EHR systems, the endpoint protection system could offer real-time visibility across healthcare structures, thus improving its capacity for identifying a large-scale security breach or a public health threat. This would enable better supervision and proper interconnection of the healthcare providers, hence enhancing the general management in the case of emergencies. In conclusion, it is vital to note that despite the proposed system provides a good beginning for

securing IoT in the healthcare sector, the improvement in the integration of devices, machine learning techniques, and the interoperability of the system in the future will greatly improve the performance and flexibility of the system. Therefore, it is a solution that can perfectly secure healthcare systems worldwide.

## REFERENCES:

1. Tang, W., Ren, J., Deng, K., & Zhang, Y. (2019). Secure data aggregation of lightweight E-healthcare IoT devices with fair incentives. *IEEE Internet of Things Journal*, 6(5), 8714-8726.
2. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). Smart contract-based access control for the Internet of Things. *IEEE Internet of Things Journal*, 6(2), 1594-1605.
3. Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*, 78, 680-698.
4. Rahmani, A. M., Gia, T. N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M., & Liljeberg, P. (2018). Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. *Future Generation Computer Systems*, 78, 641-658.
5. Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015, December). Internet of Things (IoT) security: Current status, challenges and prospective measures. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 336-341). IEEE.
6. Sharma, P. K., Chen, M. Y., & Park, J. H. (2017). A software-defined fog node-based distributed blockchain cloud architecture for IoT. *Ieee Access*, 6, 115-124.
7. Yadav, K., Alharbi, A., Jain, A., & Ramadan, R. A. (2022). An IoT-based secure patient health monitoring system. *Computers, Materials and Continua*, 70(2), 3637-3652.
8. Akkaş, M. A., Sokullu, R., & Çetin, H. E. (2020). Healthcare and patient monitoring using IoT. *Internet of Things*, 11, 100173.
9. Moosavi, S. R., Gia, T. N., Nigussie, E., Rahmani, A. M., Virtanen, S., Tenhunen, H., & Isoaho, J. (2016). End-to-end security scheme for mobility-enabled healthcare Internet of Things. *Future Generation Computer Systems*, 64, 108-124.
10. Rizvi, S., Pipetti, R., McIntyre, N., Todd, J., & Williams, I. (2020). Threat model for securing the Internet of Things (IoT) network at the device level. *Internet of Things*, 11, 100240.
11. MacDermott, Á., Kendrick, P., Idowu, I., Ashall, M., & Shi, Q. (2019, June). Securing things in the healthcare internet of things. In *2019 Global IoT Summit (GIoTS)* (pp. 1-6). IEEE.
12. Yeh, K. H. (2016). A secure IoT-based healthcare system with body sensor networks. *IEEE Access*, 4, 10288-10299.
13. Somasundaram, R., & Thirugnanam, M. (2021). Review of security challenges in healthcare Internet of things. *Wireless Networks*, 27(8), 5503-5509.
14. Samaila, M. G., Neto, M., Fernandes, D. A., Freire, M. M., & Inácio, P. R. (2018). Challenges of securing Internet of Things devices: A survey. *Security and Privacy*, 1(2), e20.
15. Salih, F. I., Bakar, N. A. A., Hassan, N. H., Yahya, F., Kama, N., & Shah, J. (2019). IoT security risk management model for the healthcare industry. *Malaysian Journal of Computer Science*, 131-144.
16. Almotairi, K. H. (2023). Application of the Internet of Things in the healthcare domain. *Journal of Umm Al-Qura University for Engineering and Architecture*, 14(1), 1-12.
17. Islam, M. M., Nooruddin, S., Karray, F., & Muhammad, G. (2022). Internet of things: Device capabilities, architectures, protocols, and smart applications in the healthcare domain. *IEEE Internet of Things Journal*, 10(4), 3611-3641.
18. Thilagam, K., Beno, A., Lakshmi, M. V., Wilfred, C. B., George, S. M., Karthikeyan, M., ... & Karunakaran, P. (2022). Secure IoT Healthcare Architecture with a Deep Learning-Based Access Control System. *Journal of Nanomaterials*, 2022(1), 2638613.
19. Binu, P. K., Thomas, K., & Varghese, N. P. (2017, September). Highly secure and efficient architectural model for IoT-based health care systems. In *2017 International Conference on Advances in Computing, communications and Informatics (ICACCI)* (pp. 487-493). IEEE.
20. Burhan, M., Rehman, R. A., Khan, B., & Kim, B. S. (2018). IoT elements, layered architectures and security issues: A comprehensive survey. *sensors*, 18(9), 2796.