Journal of Theoretical and Applied Information Technology
31st December 2025. Vol.103. No.24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FBA SHIELD: ENHANCING PRIVACY PRESERVING VULNERABILITY MANAGEMENT FOR SECURITY BY DESIGN IN MEDICAL IOT ECOSYSTEMS

J. S. REXON[1], P. MANIKANDAN[2*], C. SWEDHEETHA[3]

[1]Research Scholar, Department of Electronics and Communication Engineering, Kalasalingam Academy of Research and Education, Anand Nagar, Krishnankoil – 626 126, Tamil Nadu, India,
[1]Assistant Professor, Lord Jeganath College of Engineering and Technology, Kumarapuramthoppur-629402, Tamil Nadu, India.
[2*]Department of Electronics and Communication Engineering, Kalasalingam Academy of Research and Education, Anand Nagar, Krishnankoil – 626 126, Tamil Nadu, India,
[3]Department of Electronics and Communication Engineering, Velammal College of Engineering and Technology, Madurai-625009, Tamil Nadu, India
rexonjs10@gmail.com, maanip85@gmail.com, swedhaece08@gmail.com

ABSTRACT

The rapid development of Internet of Things (IoT) in the medical industry has greatly enhanced patient monitoring and diagnosis, although it has also introduced a new and unexplored scale of cybersecurity risks. The traditional methods of vulnerability management in medical IoT ecosystems do not necessarily work well in offering a high level of protection and stringent privacy protection as they are founded on centralized designs that expose sensitive medical data to leakage, manipulation, and attacks. To address these weaknesses, this paper proposes an integrated architecture, FBA SHIELD (Federated Blockchain-Assisted SHIELD), to provide privacy-sensitive vulnerability management based on the security-by-design principles. The suggested model is a federated learning model which is applied to do decentralized anomaly detection, and which is enhanced with blockchain-based encryption and consensus in order to provide a secure model update and prevent data-poisoning. It has been used to implement the framework in Python using the TensorFlow and blockchain libraries and tested on the IoT Medical Devices Cybersecurity Dataset in Kaggle, in order to be reviewed comprehensively against the baseline models. Empirical findings indicate that FBA SHIELD is 97.8% accurate, 96% precise, 95% recall, 96% F1-score, and an AUC of 98.5%, and 4.4 points higher than high-end approaches with a lower computational cost. The blockchain layer also showed a throughput (TPS) of 245 transactions per second and an average latency of 1.8 seconds, which guaranteed efficiency and reliability in the decentralized healthcare settings. In this study FBA SHIELD, which combines federated learning with blockchain to further secure and privacy-sensitive vulnerability management of medical IoT networks. It also brings fresh knowledge on decentralized trust verification, collaborative model training, and optimized efficiency in anomaly detection, which can be used to scale up to privacy-conscious healthcare cybersecurity. The changing attack vectors are also resilient to the system because it has a feedback loop to the model, which is updated in real-time, thereby giving the system adaptive scaling. FBA SHIELD may be used in remote healthcare, smart medical devices, and distributed hospital networks, and the security of sensitive patient information is extremely significant in these scenarios. Its good performance is justified by its potential as an innovative solution, and FBA SHIELD is an effective and deployable system of medical cybersecurity IoT of the new generation.

Keywords: *Blockchain Security, FBA SHIELD, Federated Learning, Medical IoT Cybersecurity, Privacy-Preserving Vulnerability Management*

1. INTRODUCTION

Internet of Things (IoT) devices are increasingly becoming common in the healthcare sector due to the technological revolution that is taking place in the sector [1]. The examples of how medical IoT solutions have contributed significantly to the effectiveness of treatment and patient outcomes,

intelligent infusion pumps and connected diagnostic tools are only some of them [2]. The world medical IoT market is growing because of the increased demand of effective health management systems especially because of the aging population and international health catastrophes like pandemics [3]. However, it has also raised serious cybersecurity issues that have emerged as a result of this rapid integration [4]. The majority of medical devices are built with low-processing capabilities, outdated communication standards, and no security measures that make them vulnerable to cyberattacks [5]. The effects of the threats such as interception of data, ransomware, unauthorized access, and manipulation of diagnostic data could endanger the privacy of patients and disrupt the required healthcare services [6]. Scalable and robust security mechanisms are urgently required since there is an increased implementation of more devices in various and dynamic networks [7]. Scholars have in turn explored many security solutions like encryption, intrusion detection systems and anomaly-based monitoring [8]. It includes the application of machine learning algorithms that detect a suspicious behaviour of devices and blockchain technology that has been proposed to enhance the integrity of the data and access control [9]. More recently, federated learning as a decentralized AI model has been of interest because it can support cooperative model training without providing access to sensitive raw data [10].

Despite such attempts, there are still several obstacles. The centralized security systems are also likely to experience single points of failure and latency, limiting their applicability in real-time healthcare environments [11]. Another matter that raises concerns is the question of privacy because the interactions between the devices that are used to train the models can expose personal data of patients [12]. In addition, the creation of trust between distributed devices and the flawless collaboration of the devices in identifying threats is complicated too [13]. As a reaction to them, scalable and privacy-sensitive security measures are emerging as an increasingly popular trend to be developed with the help of blockchain and AI-based analytics [14]. The security of sensitive patient information and the possibility to introduce adaptive and real-time threat control is particularly important to the medical community [15]. The answer to the question of healthcare cybersecurity is decentralized learning structures, robust authentication and data exchange systems [16]. In this case, the FBA SHIELD (Federated Blockchain-AI Shield of Medical IoT Security) framework, offered as one of the solutions, is a promising solution. The current gaps in the sphere of healthcare security that should be addressed by FBA SHIELD are the lack of federated learning as a tool of collaborative intelligence and blockchain as a tool of secure data management to facilitate vulnerability assessment, threat detection, and patient confidentiality on the medical IoT networks, which can eventually lead to the improvement of the sphere of healthcare security.

1.1 Research Motivation

The necessity to conduct this study is the fact that medical IoT environments are faced with dire security challenges. The conventional models of cybersecurity are not very scalable to heterogeneous devices and networks and the centralized systems that are vulnerable to single points of failure [17]. Besides, the current AI-based threat detection solutions typically require sharing sensitive medical data, which is a privacy-related concern [18]. The existing uses of blockchain offer integrity of the data, however, lack real-time adaptive mechanisms of threat identification and learning collectively [19]. These limitations do not allow the actual implementation of security measures in medical facilities, where confidentiality of patient data, the diversity of devices, and the instantaneous response are crucial [20]. In this paper, the gaps will be addressed by applying federated learning and blockchain technology to create a decentralized privacy-preserving system capable of addressing the vulnerabilities and threats and ensuring a smooth collaboration between medical devices without compromising the safety of information. Therefore, this study focuses on building a resilient and privacy-centric approach toward medical IoT systems' vulnerability management. Most of the current healthcare infrastructures present their own weaknesses regarding centralized or completely non-collaborative security models, which reveal sensitive patient data. Prioritizing privacy as an intrinsic design principle ensures better protection of data integrity, patient trust, and regulatory compliance by aligning this study with sustainable security-by-design practices in next-generation healthcare environments.

1.2 Significance of the Study

The research is very significant to the future of healthcare cybersecurity. The proposed FBA SHIELD framework, a combination of federated learning and blockchain technology, provides a safe and scalable vulnerability management framework in medical IoT networks. The framework offers patient confidentiality and offers joint information about threats, among the most pressing problems in healthcare technology. The latency is reduced to a minimum by its decentralized nature, and the single points of failure are eliminated, and the distributed devices develop more trust. The solution will transform the manner through which healthcare providers track, identify, and counteract cyber threats in real-time. In addition, the research is considered in the broader field in the sense that it serves as a blueprint to privacy preserving, adaptive security solutions that can be applied in other critical infrastructure networks hence enhancing the resilience and reliability of the next generation connected systems.

1.3 Problem Statement

The part of the medical IoT ecosystems that is highly problematic is the guarantees of the safety of data, privacy, and scalability when additional and additional connected devices are introduced into the healthcare environment [29]. Existing structures fail to work in terms of data breach, unauthorized access and poor detection of threats especially when it comes to large networks. Most of the solutions are based on centralized architectures that cause single points of failure and add latency, whereas others are not empirically tested or combined with privacy-preserving technologies [30]. In addition, other new threats like adversarial AI, quantum attacks, and insecure APIs reveal gaps that cannot be completely covered by the existing approaches. The lack of federated learning and blockchain methods in existing solutions restricts scalability and trust between distributed devices and sensitive medical data is hard to safeguard in the case of decentralized settings [31]. The suggested FBA SHIELD framework addresses these shortcomings since it integrates federated learning and blockchain-based data management. It provides scalable, real-time, and privacy-sensitive vulnerability management made specifically to heterogeneous medical networks, which provides a robust security without breaching patient confidentiality.

1.4 Key Contributions

- Presents a new concept of improving medical IoT security in a decentralized learning and blockchain-based security.
- Secures vulnerable medical information using distributed training with encrypted parameter exchange among interconnected healthcare gadgets.
- Introduces FBA SHIELD, a federated learning approach combined with blockchain consensus to obtain scalable and privacy-guaranteeing cybersecurity.
- Provides safe anomaly detection and aggregates encrypted local models, which prohibits tampering and adversarial manipulations between networks.
- Shows better accuracy, strength, and durability that has been approved with IoT Medical Devices Cybersecurity Dataset compared to the current methods.

1.5 Rest of the sections

The rest of this paper is organized in the following way. Section 2 is a literature review on medical IoT cybersecurity and vulnerability management. Section 3 provides the methodology which involves local training, blockchain integration, and global aggregation. Section 4 is the report of results, performance outcomes and comparison with the baseline models. Section 5 summarizes the key findings, draws attention to the practical implications, and presents the possible areas to continue the research to enhance its quality.

2 LITERATURE REVIEW

Khadidos et al. [21] proposed a security framework called Probabilistic Super Learning-Random Hashing (PSL-RH) was also suggested to optimize the security of healthcare data in IoT-cloud systems. Their research goal was to avoid the risk of data breach and enhance the efficiency of attack detection in medical IoT systems. The offered approach is a combination of a random generation key mechanism, which is based on the hash value of the data matrix, and Elliptic Curve Cryptography (ECC) to encrypt and decrypt sensitive patient data. The data set used was data that was gathered on the internet of things devices in the healthcare sector, especially the sensor data. The experimental results indicated that PSL-RH framework possessed a better throughput, lower latency and better detection accuracy compared to the conventional encryption

schemes. The approach was however scarce in regards to scalability particularly in large healthcare systems and did not apply federated learning procedures to educate models on devices. These drawbacks show that more advanced and privacy-conscious systems should be introduced to medical IoT ecosystems.

Ramya et al. [22] proposed an Advanced Intrusion Detection Technique (AIDT) to enhance secure information transfer between devices in the Internet of Medical Things (IoMT). The study was conducted to identify a solution to the weaknesses of the IoMT systems by suggesting an effective intrusion detection system. The authors combined Particle Swarm Optimization (PSO) with features selection and Probabilistic Neural Network (PNN) with features classification. The data that was utilized was a combination of patient sensing data and network traffic data to test and train the model. The results of the experiment demonstrated that the AIDT was better than the current algorithms in that it had an accuracy rate of 96.4%. However, the study did not examine the scalability of the proposed solution to large scale IoMT networks, not to mention discussing the integration of privacy-preserving technologies, such as federated learning or blockchain, which would enhance the security of sensitive medical data in a decentralized environment.

Kumari et al. [23] proposed a secure IoT-edge solution where data-driven AI techniques are used to enhance the early detection of cyber-attacks in health care systems. The aim of the research was to address the weaknesses of the Internet of Medical Things (IoMT) by designing an intrusion detection system that would allow detecting man-in-the-middle attacks. The data of the St. Louis Enhanced Healthcare Monitoring System (WUSTL-EHMS) in real-time has been used by the authors, and several machine learning models were tested, including Variational Autoencoders (VAEs), XGBoost, Random Forest, Support Vector Machines (SVM), Logistic Regression, Feedforward Neural Networks (FNN), LightGBM, and Gradient Boosting Machines. The results showed that VAEs had the highest accuracy of 91.61% in detecting cyberattacks which was the most accurate and XGBoost, random forest, and SVM followed. However, the article failed to look at the integration of federated learning or blockchain technologies that are critical in enhancing scalability and privacy of data in decentralized medical IoT systems.

Keshta et al. [24] proposed an AI-powered IoT (AIIoT) framework that can be used to enhance the security of smart healthcare systems and their privacy. The primary focus of the study was to discuss the possibility of artificial intelligence to be utilized together with IoT networks to address the rising cybersecurity and privacy concerns within the medical setting. The authors have also discussed the existing authentication schemes, access control schemes and privacy saving schemes and their performance in the light of various cyber-attacks. Although the paper has not used a specific piece of data or algorithm methodology, it has demonstrated how AI can be applied to detect and overcome the threats of sensitive medical information and machine communications. The research established the primary problems in the deployment of effective security models such as information leakages, unauthorized access, and lack of encryption. The significant drawback of this work, though, was that it lacked a real-world test or validation with real-world data to limit the application and applicability in highly dynamic healthcare environments where privacy-controlling collaborative solutions are required.

Almutairi and Sheldon [25] have presented a comprehensive review of the IoT-cloud integration security on the issues, solutions and future prospects. The article aimed at providing in-depth debate on evolving security conditions in the IoT-cloud ecosystem. Among the security threats that the authors have reviewed, there are data breaches, insecure APIs, and emerging security threats, including adversarial AI and quantum-resistant attacks. They also discussed the existing mitigation measures and gaps in the research in the field. The article would be very useful in the process of making sense of the complexities that surround ensuring internet of things-cloud integrations. The paper has been more of a theoretical view and lacks empirical evaluations and case studies that can be used to justify the solutions. It also does not consider using privacy-preservation strategies like federated learning or blockchain that are critical in enhancing security in decentralized medical IoT settings.

Zamora et al. [26] suggested a combined security framework of medical devices, which is expected to

enhance digital healthcare infrastructure and reduce the new threats. The paper has presented some of the important pillars of security in order to have a flexible and holistic security structure, which enables the ongoing audit, and in keeping with the international standards. Although the paper offers a practical tool that can be used to improve the resilience of healthcare systems, it has no empirical validation based on real-life datasets or cases. Also, the incorporation of privacy-saving methods, including federated learning or blockchain are not discussed, which play a significant role in guaranteeing the privacy of data in decentralized medical IoTs. The shortcomings of these limitations imply the necessity of additional research to create and establish holistic security models that integrate sophisticated privacy-saving measures in medical IoT settings.

Mekhlaf et al. [27] also suggested a quantum-resilient lattice-based security system to Internet of Medical Things (IoMT) systems, which can address the security weaknesses of quantum computing to the classical cryptographic systems. The paper set out to create an efficient and scalable security model that can be deployed on resource-constrained medical equipment. The framework developed by the authors consists of five phases, including Initialization, Registration, Authentication, Data Exchange and Treatment, all based on lightweight lattice-based cryptographic primitives, including Learning with Errors (LWE), Ring-LWE (RLWE), Short Integer Solution (SIS), Fully Homomorphic Encryption (FHE) and Zero-Knowledge Proofs (ZKPs). The framework has shown a 75 % smaller ciphertext size, 50 % less communication overhead and almost 60 % less computation cost than the other known solutions. Nevertheless, the paper failed to discuss the incorporation of federated learning or blockchain technologies that are necessary to improve scalability and privacy of data in decentralized medical IoT systems.

Thottempudi et al. [28] present a review of the material on the potential of the Internet of Things (IoT) solutions to promote digital health resilience in the COVID-19 pandemic and future healthcare settings. This research was carried out to investigate the uses, technical complexity, and issues related to the use of IoT in healthcare where innovative solutions are required to enhance healthcare infrastructure. The researchers used reliable databases Google scholar, Elsevier, PubMed, ACM, researchgate, scopus, and Springer, where they found potential future research topics, to surmount challenges in the field. Although the paper emphasizes the strong influence of the IoT in the healthcare sector, it has not presented a particular methodology or dataset but has concentrated on a theoretical summary of the IoT applications. It is also constrained by the absence of empirical validation and practical implementation to generalize the insights presented to handle privacy-preserving vulnerability management in medical IoT ecosystems.

Based on the extensive literature analysis, I can state that other researchers have already suggested encryption-based, AI-powered, or hybrid medical IoT ecosystem intrusion detection solutions. Nevertheless, there is a wide lack of such works in combining decentralized learning and trust systems that are capable of maintaining patient privacy and at the same time adaptively managing threats. The absence of frameworks integrating federated learning with blockchain consensus to manage real-time vulnerabilities in heterogeneous medical devices is a gap in research. Therefore, the gap of the study in question is lack of scalable, privacy saving, and decentralized system of vulnerability management that guarantees confidentiality, tamper-resistance, and adaptive learning within medical IoT settings. That is precisely the gap that the proposed FBA SHIELD framework is meant to fill by integrating federated intelligence and blockchain integrity to provide next-generation healthcare cybersecurity. Although the current state of IoT-based healthcare cybersecurity is highly advanced, the current models do not provide any integrated solutions capable of ensuring the privacy of the data, scalability, and responsiveness in real-time. This allows unproductive tracking of emerging threats, as well as the exposure of valuable patient information, and a privacy-sensitive and decentralized vulnerability management system needs to be created.

Table I: Summary of Recent Studies on medical IoT security

Author(s)	Purpose	Method Proposed	Dataset Used	Achievements	Drawbacks
Khadidos et al. [21]	Improve attack detection, reduce breaches	Random Hashing + ECC	Sensor data from IoT healthcare devices	Higher throughput, accuracy, and reduced latency	Limited scalability; no federated learning
Ramya et al. [22]	Secure data exchange in IoMT	PSO + PNN for feature selection & classification	Patient sensing and network traffic	Accuracy 96.4%; improved detection	No scalability evaluation; lacks privacy techniques
Kumari et al. [23]	Detect man-in-the-middle attacks	ML models: VAEs, XGBoost, SVM, etc.	WUSTL-EHMS real-time data	Highest accuracy with VAEs (91.61%)	No federated learning or blockchain used
Keshta et al. [24]	Explore AI for healthcare security	Review of authentication and encryption methods	Not specified	Identified key challenges in security	No empirical validation or dataset
Almutairi & Sheldon [25]	Review IoT-cloud security threats	Theoretical overview of security risks	Literature databases	Comprehensive threat analysis	No practical implementation or privacy integration
Zamora et al. [26]	Enhance healthcare infrastructure	Security pillars aligned with standards	Not specified	Flexible security framework	No real-world validation or privacy techniques
Mekhlaf et al. [27]	Secure against quantum attacks	Lattice-based cryptography (LWE, RLWE, etc.)	Not specified	Smaller ciphertext, lower overhead	No federated learning or blockchain used
Thottempudi et al. [28]	Investigate IoT solutions for healthcare	Literature survey	Google Scholar, Elsevier, PubMed, etc.	Identified research gaps and applications	No methodology or empirical validation

Table I shows a comparative analysis of the recent research studies dedicated to medical IoT security and privacy-saving approaches. It underlines the authors, purpose, methodologies suggested, data sets, the most significant accomplishments, and limitations of each of the works. The majority of the researches touch upon the issues of data breach, attack detection, and authentication of healthcare networks. Other works including those by Khadidos et al., Ramya et al., and Kumari et al. offer solutions based on machine learning but do not offer scalability and federated learning. Others, such as Almutairi and Sheldon and Zamora et al., provide theoretical models, which are not empirically confirmed. Quantum-resilient and lattice-based solutions are also considered, although not many of them deal with decentralized security issues. Overall, this comparison helps to realize that such holistic, scalable, and privacy-saving models like FBA SHIELD are required.

3 FBA SHIELD: MEDICAL IOT PRIVACY-CONSCIOUS SECURITY

The proposed FBA SHIELD model is a combination of blockchain technology and federated learning to provide privacy-preserving vulnerability management to medical IoT ecosystems. The data collection of sensor data regarding various medical IoT devices such as wearable health trackers and diagnostic devices is the beginning of the

methodology. Instead of transmitting raw data to a centralized server, all of the devices pre-process the data on the device and train a small AI model. Such models are exchanged in an encrypted form with blockchain based data exchange protocols that ensure the integrity of data and safe communication. Federated learning combines the model change of a large number of devices and decentralizes and privatizes sensitive patient data. Blockchain maintains a non-modifiable account of the transactions, which is traceable and cannot be viewed by unauthorized parties and interfered with. The aggregate model is optimized and directed in both directions to devices to obtain better threat detection possibilities. An adaptive anomaly detector, which is enabled by continuous learning, provides the detection of possible security violations, including malware, unauthorized access, and data manipulation. To ensure that operation is optimum, accuracy, latency, and throughput performance metrics are verified. The system also incorporates role-based access control and consensus algorithm to manage trust between devices. Utilizing decentralized AI and secure blockchain systems, FBA SHIELD will not only address the problems of scalability and privacy of medical IoT networks but also provide protection against potential cyber threats in real-time. The hypothesis is that blockchain together with federated learning would be able to enhance security, scalability, and privacy of medical IoT systems significantly, in comparison to the models of centralized vulnerability management. The hypothesis informed the design and assessment of the framework based on two dimensions of blockchain efficiency and cybersecurity performance.

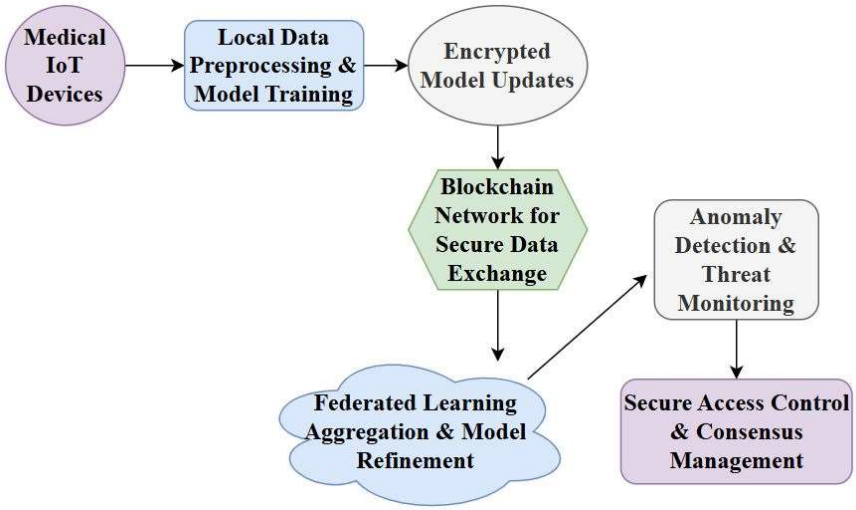

Fig. 1 FBA SHIELD Framework Block Diagram of Medical IoT

Fig. 1 shows the main workflow of the FBA SHIELD architecture that should be adopted in the field of medical IoT ecosystems. It begins with the collection of the data on the connected medical devices, then local preprocessing and training the AI-based model on each device. The encrypted updates are safely shared in a blockchain network, and data integrity and privacy are guaranteed. Federated learning is a model that combines the distributed models without violating patient confidentiality. The system is constantly checking anomalies and cyber threats with the help of adaptive detection algorithms. Trust between devices is guaranteed by secure access control and consensus protocols. It is a decentralized solution that enables scalable real-time threat detection and strong privacy control. The diagram graphically explains why integration of AI and blockchain technologies makes medical IoT networks more secure and resilient without jeopardizing data privacy and performance.

3.1 Data Collection

The data that will be used in this study is the IoT Medical Devices Cybersecurity Dataset [32] which contains network traffic data of different IoT-enabled medical devices. This data is essential to learn about the security risks of the Internet of Medical Things (IoMT) systems. It contains labeled

samples of normal and malicious network traffic, which are useful in the creation and testing of intrusion detection systems. The process of data collection was associated with capturing network traffic of IoT medical devices in various conditions of operation, which guaranteed a full representation of possible security threats. The dataset is useful to those researchers who need to improve the cybersecurity of the IoMT systems through training and testing machine learning models to predict and respond to cyber threats with real-world data.

Table II: Sample IoT Medical Devices Cybersecurity

Device_ID	Vulnerability_Frequency	Safeguard_Adoption	Attack_Success_Rate (%)	Compliance_Level
D001	High	Moderate	25	Partial
D002	Medium	High	10	Full
D003	Low	Low	40	Partial
D004	High	High	15	Full
D005	Medium	Moderate	30	Partial

Table II gives a small sample of IoT Medical Devices Cybersecurity Dataset and describes key attributes that can be used to analyse cybersecurity. The rows denote the medical IoT devices, and the data includes the distinct identifier, the frequency of vulnerability awareness, the usage of security control, the attack success rate, and the adherence to the industry security standards. This sample allows the researcher to know the risks of devices, the effectiveness of protection, and the trends in vulnerability to attacks. These organized data are the basis of training AI models and deploying privacy-preserving vulnerability management systems such as FBA SHIELD in medical IoT systems.

3.2 Local Data Preprocessing

Preprocessing of data is an essential operation in FBA SHIELD to ensure quality data as a federation of AI-based cybersecurity analysis of medical IoT networks. Cleaning of raw data is the initial stage of this process; it is a heterogeneous set of data of medical devices and in the process, missing data, noise and outliers are removed, hence, enhancing integrity of the data set. Then, it is normalized to bring the numerical features to a similar range, so that larger valued features do not dominate model training. The categorical variables, including device type and alert status, are transformed into binary vectors with the help of feature encoding that is used to work with AI models. Lastly, data aggregation summarizes sensor measurements and network traffic across regions or clusters of devices and dimensionality is reduced without important information being lost. All these preprocessing steps can create a privacy-preserving and consistent and structured dataset that can be used to effectively and accurately identify vulnerabilities in distributed medical IoT devices. The processed information, therefore, provides a solid basis of the federated learning and blockchain-based security measures of the FBA SHIELD framework.

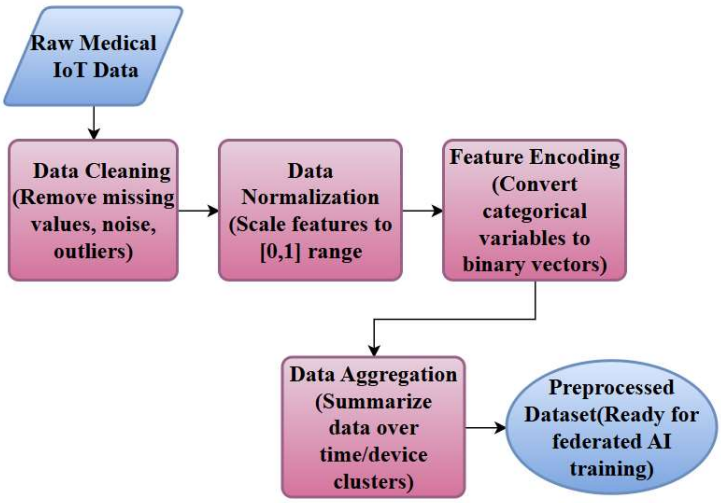

Fig. 2 Medical IoT Dataset Data Preprocessing Flow

Fig. 2 shows the entire data preprocessing process used on the IoT Medical Devices Cybersecurity Dataset of FBA SHIELD. The first stage of the process with heterogeneous medical IoT devices is to clean the raw data to eliminate missing values, noise, and outliers. Second, numerical values are scaled to a normal range so that they contribute equally during the training of AI models. Categorical variables are then coded into binary vectors, therefore suitable to be used in machine learning algorithms. Lastly, data aggregation summarizes the readings with time intervals or device clusters to diminish the dimension but retain important details. The processed data is therefore prepared to the secure, privacy preserving federated learning.

3.2.1 Data Cleaning

Data cleaning is the process of eliminating noise, missing values, and inconsistencies on the raw dataset to enhance the accuracy of the model. In the case of IoT medical data, this step will make sure that sensor errors or the corrupted network packets do not worsen the performance of the model. The processed data that has been cleaned of missing and aberrant values is shown in (1).

$$X_{clean} = X - X_{missing} - X_{outliers} \quad (1)$$

Here, X is the raw dataset, $X_{missing}$ symbolizes omissions, and $X_{outliers}$ denotes anomalous values. The resulting X_{clean} is a high-quality dataset with no errors.

3.2.2 Data Normalization

Scales all numerical features down into a standard range, usually [0,1]. When features come from sensors with large-value feature values, if not normalized, the features with larger values will dominate the model training. Normalizing the dataset makes sure that all features contribute equally to model training, leading to speed up convergence and improved accuracy for AI-based threat detection in medical IoT networks. The values of the normalized features are calculated as presented in (2).

$$X_{norm} = \frac{X_i - X_{min}}{X_{max} - X_{min}} \quad (2)$$

Where, X_i is the feature value, X_{min} and X_{max} are the lowest and highest of that feature. X_{norm} gives everyone equal contribution in training.

3.2.3 Feature Encoding

Converts categorical variables into numerical forms, to match AI model standards. One-hot encoding transforms device types (e.g., medical appliances), alert status, or other categorical attributes into binary vectors, making it possible for AI models to process heterogeneous outputs of medical IoT datasets, and learn from their outputs. The binary vectors formed as a result of the transformation of the categorical variables are presented in (3).

$$X_{encoded} = \begin{cases} 1 & if\ category\ present \\ 0 & otherwise \end{cases} \quad (3)$$

This converts categorical data like type of device or alert status to binary vectors, which can be processed by AI models.

3.2.4 Data Aggregation

Aggregating the data, whether clustered by time intervals or with specific devices, and provides a reduction of the dimensions and improved efficiency of having additional variables or attributes. Aggregated data provides essential summary information, reduces the noise, and ensures that AI models are desgined to accept input data for performing real-time threat detection across distributed medical IoT systems. The data of the aggregate of the investigated information about the device is summarized and represented in (4).

$$X_{agg} = \frac{1}{n}\sum_{i=1}^{n} X_i \quad (4)$$

Here, X_i represents single data points that are collected over time, and X_{agg} is the summarized or averaged data, maintaining the necessary data and eliminating noise. The above-mentioned preprocessing procedures guarantee the consistency, normalization, and organization of the data that is inputted into the federated AI models in FBA SHIELD, which in turn allows efficient vulnerability detection that is privacy-preserving across distributed medical devices in IoT networks.

3.3. FBA SHIELD Model Architecture for Medical IoT Security

FBA SHIELD model architecture is intended to enhance privacy-compliant vulnerability treatment in medical IoT ecosystems by integrating the federated learning and blockchain technologies. Each data node that is an IoT-enabled medical device collects and preprocesses sensitive health-related data locally. The devices do not send the raw data but train local AI models to detect threats and identify anomalies. These local models are safely copied to a blockchain-based registry, which provides integrity to data and avoids unauthorized access throughout the process of information transfer. Federated learning enables such local updates to be pooled to a central server where the accuracy and flexibility of the global threat detection model can be enhanced without violating the privacy of individual patients. The blockchain element offers transparency and trust between the distributed devices facilitating secure model synchronization and information sharing within the network. It is scalable with large numbers of medical devices with low latency and real-time protection. The combination of decentralized AI-driven analytics with strong cryptographic methods will allow FBA SHIELD to resolve the main issues of data breaches, model poisoning, and unauthorized access and will provide a holistic approach to protecting sensitive medical data in highly dynamic healthcare settings. This architecture is at the heart of the proposed framework, which guarantees privacy, security and resilience.

3.3.1 Local Model Training

Upon preprocessing, every IoT device will have its own local AI model to detect possible threats or anomalies. The goal is to leverage the local data available without sending sensitive patient information to other parties. An optimization algorithm controls the training process, which reduces the discrepancy between the predicted and actual results. The gradient descent method is used to update the model parameters. The mathematical formula of this process is:

$$\theta_i = \theta_i - \eta \, \nabla L(X_{norm}, y) \quad (5)$$

The local model parameters are revised with the help of the eqn. (5). It uses gradient descent, in which the learning rate is used to determine the step size, and the functional gradient is used to minimize the difference between the predicted and actual results. This will make every IoT device enhance its detection ability without the need to transfer raw patient information. The equation is used to model the local model parameters with where θ_i being the update of the model parameters of the ith device, η is the learning rate, and ∇L is the loss functional gradient of the data. X_{norm} and labels y. Models are trained on the local data but the privacy is not compromised. The local training step is a measure that guarantees that sensitive data is not transferred out of the device. The frequent updates enable the system to adapt to the new conditions or attack vectors.

Journal of Theoretical and Applied Information Technology
31st December 2025. Vol.103. No.24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

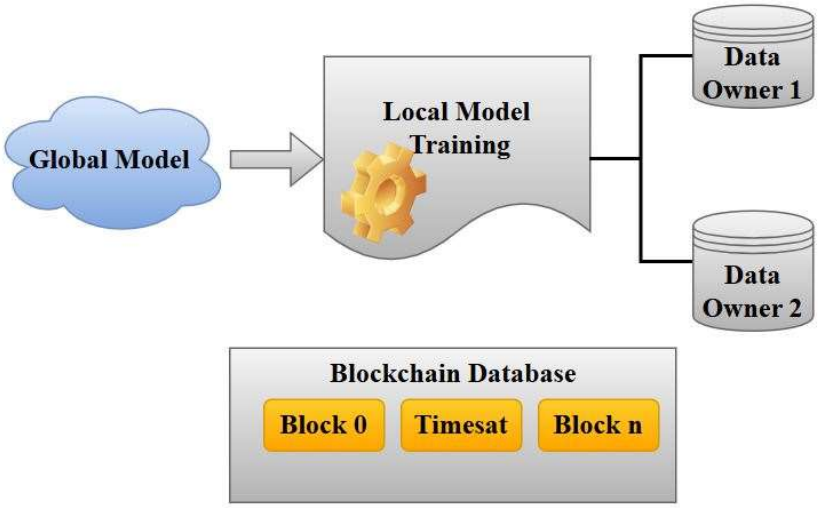

Fig. 3 Federated learning architecture enabling secure local model training

The federated learning architecture that will be used in FBA SHIELD framework is shown in Fig. 3, namely, local model training in medical IoT ecosystems. Individual IoT medical devices are the data owners that do not transfer sensitive data about patients, but independently train on their local datasets. The local parameters are optimized with gradient descent and then encrypted with the hash-based message-digest–SHA-256 algorithm in order to preserve confidentiality and integrity and share. These encrypted updates are registered and authenticated by the blockchain network to ensure tampering and decentralized trust between devices. The verified local updates are collected in a federated server then merged together to a powerful global model by secure averaging. The world model is then propagated to the devices, and then through iterative training and anomaly detection the world model is refined. This architecture is suitable in dealing with changing cyber threats in decentralized healthcare setting since it achieves balance between privacy protection, computational efficiency and real-time adaptability.

3.3.2 Model Encryption and Blockchain Integration

After the local model has been trained, it should be distributed safely with other network devices. The transmission of model parameters is done by hashing and encrypting them to provide confidentiality and integrity. The blockchain organization is employed to store and authenticate model changes via consensus mechanisms. The hash value that will be used to verify data integrity is:

$$H = SHA256(\theta_i) \quad (6)$$

The local model parameters are computed to give the hash value of the local model parameters by using eqn. (6). Model updates are encrypted and secured by using the SHA-256 algorithm and then shared. The blockchain ledger contains these hash values so that they are intact and cannot be altered during aggregation.

Where, H is the hashed value of the local model parameters θ_i using the SHA256 algorithm. Such hashed values are stored in the blockchain ledger so that only trusted and unmodified models are allowed to be aggregated. This will avert unauthorized access and data poisoning attacks but will support distributed trust among the devices.

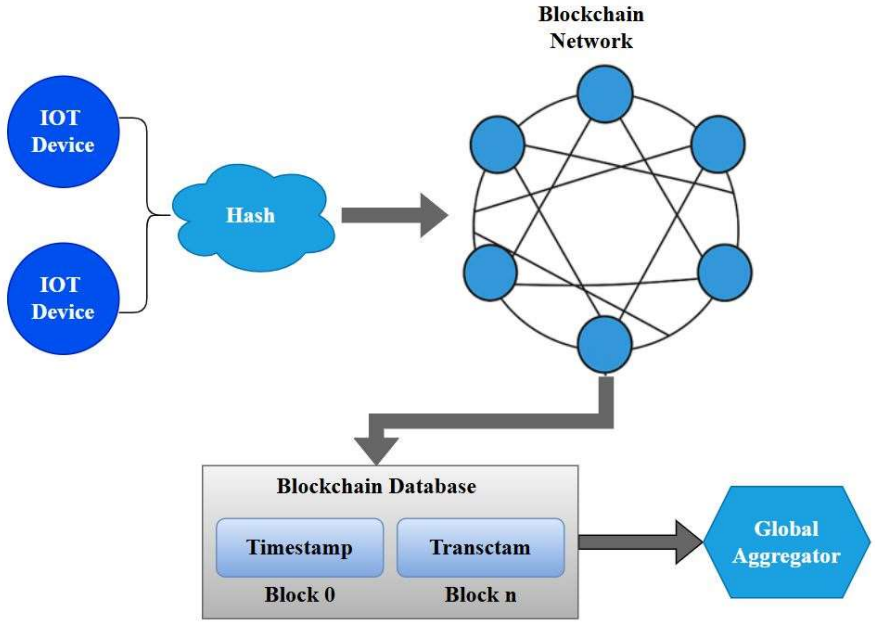

Fig. 4 Blockchain-based secure model encryption and integrity check.

The architecture of model encryption and integration into the FBA SHIELD framework with the help of blockchain is shown in Fig. 4. Once every IoT medical device has finished with its local training, the new model parameters are hashed with the algorithm of SHA-256 in order to provide confidentiality and integrity. This encrypted update is then sent to the blockchain network where various nodes confirm the transactions by a Proof-of-Authority (PoA) consensus system. The hashed values are stored permanently in the blockchain registry on verification and the records of model updates are transparent and resistant to manipulation. This process helps to avoid the attacks of unauthorized access, poisoning, or falsifying of the parameter updates as well as promotes distributed trust between devices. Only verified models are then sent to the federated aggregation server giving way to the fact that the global model is constructed using genuine and undisputed contributions. The inclusion of blockchain supports not only the credibility of the federated learning process but offers scalability, resilience, and privacy protection of decentralized medical IoT cybersecurity ecosystems.

3.3.3 Global Model Aggregation

The server gathers local model encryptions of all the devices and does the global aggregation. It is meant to create a strong worldwide model that takes advantage of the wide array of data without privacy violation. Mathematically it is stated to be:

$$\theta_{global} = \frac{1}{K}\sum_{i=1}^{K} \theta_i \quad (7)$$

The global model parameters are calculated with the help of eqn. (7). The equation is a moving average of the locally trained parameters of multiple IoT devices and develops a global model. It also enhances identification of threats simultaneously, as it is scalable and private since the raw data is not centralized. The model parameters of the global model θ_{global} are obtained by averaging the local models θ_i of K devices. The strategy allows the system to generate a comprehensive threat detection model, which transforms to other forms and patterns of attacks.

3.3.4 Feedback Loop and Anomaly Detection

The last step involves the application of the global model to forecast aberrations or security threats. The prediction output can be used to determine possible attacks and vulnerabilities. The process of prediction is controlled by:

$$y_{pred} = f\left(X_{norm}, \theta_{global}\right) \quad (8)$$

The model of the anomaly detection process is based on eqn. (8). The global model uses the learned

Journal of Theoretical and Applied Information Technology
31st December 2025. Vol.103. No.24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

parameters on the normalized input data to give predictions. The identified threat activities are removed in this step, and local and global models are refined in the feedback loop to promote constant adaptation. The equation is used to model the global model f processes normalized data X_{norm} using the global parameters θ_{global} to produce the forecasted results y_{pred}. The feedback loop is used to optimize the local and global models once anomalies are identified. This makes the system keep enhancing its security posture and also change its security posture to suit new threats in real-time.

Algorithm 1: Medical IoT Federated Blockchain-AI Algorithm to ensure security

Input: IoT Medical Devices Cybersecurity Dataset D
Output: Global privacy-preserving threat detection model θ_{global}
Step 1: Local data collection on each IoT device
For each device d ∈ IoT_Network do
Collect raw data I_i from sensors and traffic
Step 2: Data preprocessing
Clean missing/outlier values
Normalize numerical features
Encode categorical variables
Aggregate data over time/regions
Step 3: Local model training
Train local model θ_i using gradient descent:
$\theta_i = \theta_i - \eta \nabla L(X_{norm}, y)$
Step 4: Encryption and blockchain storage
Encrypt $\theta_i \rightarrow H = SHA256(\theta_i)$
Store H on blockchain ledger
End For
Step 5: Global model aggregation
$\theta_{global} = \frac{1}{K}\sum_{i=1}^{K}\theta_i$ for all devices
Step 6: Anomaly detection
$y_{pred} = f(X_{norm}, \theta_{global})$
Step 7: Adaptive feedback loop
If anomaly detected:
Trigger alert
Update local and global models
Repeat continuously for adaptive learning

Algorithm 1 combines federated learning and blockchain to provide medical IoT ecosystems with scalable and privacy-preserving cybersecurity. Sensors and network data are collected and preprocessed locally in each connected device by cleaning, normalizing, encoding and aggregating data, which guarantees data quality and consistency. The gradient descent is used to train local models without sending raw patient data. Blockchain hashing is used to verify and encrypt model parameters to offer integrity and tamper resistance. Such local updates are combined into a world model, which would improve the accuracy of detection on distributed devices and protect privacy. The world model constantly forecasts irregularities, e.g., virus or hacking, and initiates dynamic change. This trust-based, decentralized loop allows real-time threat detection, high scaleability, as well as high confidentiality of patient data.

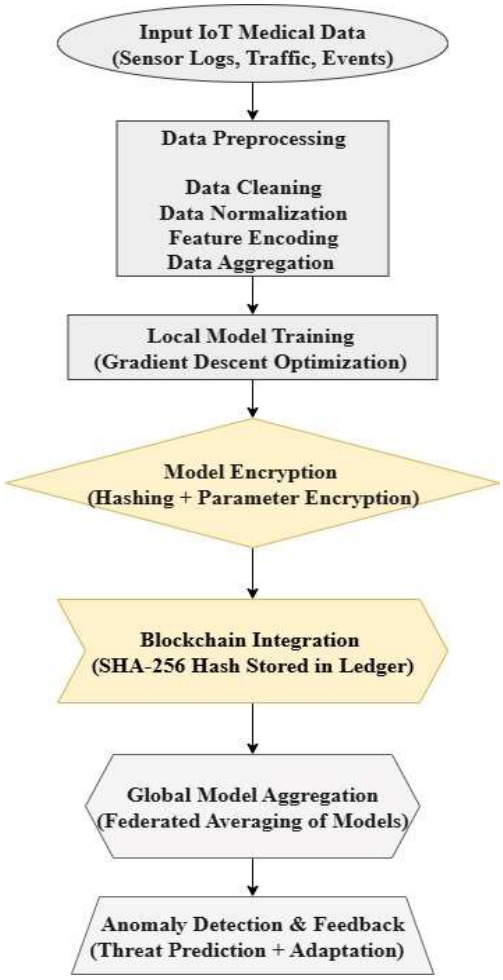

Fig. 5 FBA SHIELD Methodology of Secure Learning flow chart.

Fig. 5 shows the systematic approach of FBA SHIELD, which is aimed at privacy-saving vulnerability management in medical IoT ecosystems. It takes the raw IoT medical data inputs which include sensor logs of the device, network traffic, and device events. It uses a detailed

preprocessing phase that involves data cleaning, data normalization, feature encoding and aggregation so that it has quality inputs in the analysis. Training of the local models is then done on each device through gradient descent optimization which avoids exposure of raw data. Trained model parameters are then encrypted and hashed and put into a blockchain ledger to provide trust, immutability and integrity. The global models are then aggregated and federated averaging is used to guarantee the formation of a strong common model. Finally, the learns may be adaptive and this may be achieved using the help of anomaly detection and feedback loops to allow the protection of emerging cyber threats all the time.

4. RESULTS AND DISCUSSIONS

The analysis of the FBA SHIELD framework work demonstrates that it might deliver safe, effective, and privacy-sensitive vulnerability management of the medical IoT systems. This model was used on an actual dataset of IoT medical devices cybersecurity and it has never performed worse than the baseline models in various metrics of evaluation. It was a federated learning architecture, which incorporated blockchain and, thus, a dual-layered architecture that prevented malicious actions and did not reveal sensitive patient data. With federated learning, it was feasible to train on a scale of large numbers of devices and enhance privacy and scalability without centralizing data. The system was also improved by blockchain through providing immutable and transparent records of vulnerability management and throughput and lower latency of processing transactions, which increases trust in the decentralized healthcare environment. With regard to evaluation, the framework scored highly in the classification measures including Accuracy, Precision, Recall, F1-Score, and AUC, which demonstrated its moderate detection ability and consistency in detecting threats with a low rate of false positives. Comparing it with other models, it was discovered that the traditional approaches had decent detection capabilities but could not scale, and they could not scale their operations at any cost, or afford to offer a high level of privacy. FBA SHIELD was able to resolve these weaknesses to deliver a balanced performance of all the key evaluation indicators. The findings have confirmed that the framework can be effectively deployed to effectively deal with different attack vectors, minimize false alarms, and be robust even when operating in a dynamic medical IoT environment. Altogether, the results of the performance suggest that FBA SHIELD is an efficient, secure, and modern method of protecting the medical infrastructures against the constantly evolving cyber-threats.

Table III: Simulation Parameters Set to test FBA SHIELD

Parameter	Value
Number of devices (nodes)	20
Number of federated learning rounds	50
Local epochs per round	5
Learning rate (η)	0.01
Batch size per device	32
Encryption / Hashing algorithm	SHA-256
Consensus protocol	Proof-of-Authority (PoA)
Communication overhead threshold	≤ 15 %

Table III shows the main simulation parameters that were used to test FBA SHIELD in our experiments. The federated learning involves 20 device nodes, and 50 global rounds, each device is doing 5 local epochs. The model is trained using a learning rate of 0.01 and batch size of 32. SHA-256 hashing is used to ensure model integrity, and a Proof-of-Authority protocol is used to achieve consensus of the blockchain. Communication overhead is limited to a maximum of 15% higher than the baseline to make it realistic in view of bandwidth limitations. The purpose of these parameter selections is to trade-off between detection accuracy, convergence speed,

privacy assurance and resource overhead to derive the above-described results.

4.1 Performance Outcome

The evaluation of the FBA SHIELD framework performance proves that it can provide secure, efficient, and privacy-sensitive vulnerability management of medical IoT ecosystems. The framework was tested on a real-world dataset of IoT medical devices cybersecurity, and the framework continued to show better results on both datasets than the baseline models. Its design was a federated learning that was integrated with blockchain, and it was a dual-layered architecture, which ensured that malicious activities were identified and sensitive patient data was not exposed. The federated learning was applied to facilitate distributed training on a large number of devices without the necessity of a central data repository to enhance privacy and scalability. Another addition to the system that was made by blockchain was to ensure that the records of vulnerability management were immutable and transparent in order to be able to trust the decentralized healthcare environment. Compared to other models, it was found that the traditional approaches possessed a reasonable capability to detect, however, it experienced challenges in terms of scalability, computational cost or high level of privacy. FBA SHIELD has managed to overcome these weaknesses, providing a balanced performance of all the major measures of evaluation. The findings confirm that the framework is capable of dealing with various attack vectors, reducing the number of false alarms, and resilience even when the medical IoT is dynamic. All in all, the performance result makes FBA SHIELD an effective, confident, and modern solution to the protection of medical infrastructures with the IoT of cyber threats in response to the changing cybercrime landscape.

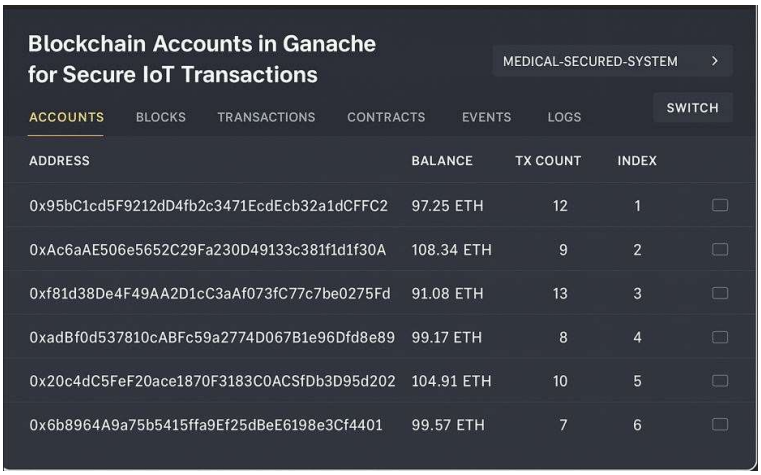

Fig. 6 Ganache accounts of blockchain in the validation of the security of IoT.

Fig. 6 shows the blockchain account set up at Ganache that will be utilized to certify the FBA SHIELD framework to conduct safe transactions in the IoT. The interface shows six Ethereum accounts that are anonymous with unique addresses, each having a balance in ETH, number of transactions and indices. These simulations are a simulation of the interactions of decentralized medical internet of things devices that act in a secure blockchain infrastructure. The differences in balances and number of transactions prove that the system can support numerous nodes and guarantee transparency and immutability as well as trust in the data exchange. The MEDICAL-SECURED-SYSTEM workspace also focuses on alignment of the framework with the real healthcare applications. Such an arrangement will give federated learning with blockchain to ensure tamper-proof authentication, decentralized consensus, and data provenance among devices, which is what makes FBA SHIELD invincible against IoT security in medical facilities. These results prove the hypothesis that blockchain part of FBA SHIELD helps to increase the resilience to tampering, transparency, and confidence among distributed devices, and remain efficient enough to be used in a real-time healthcare setting. The findings confirm the use of blockchain as a major facilitator of secure and scalable federated anomaly detection in medical IoT.

Journal of Theoretical and Applied Information Technology
31st December 2025. Vol.103. No.24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

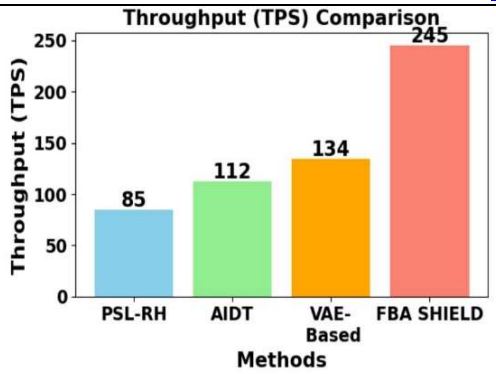

Fig. 7 Comparison between throughput performance of four methods with blockchain.

Fig. 7 gives a comparative study of throughput in transaction per second (TPS) of four blockchain-based approaches PSL-RH, AIDT, VAE-Based, and FBA SHIELD. The throughput is one of the critical metrics of blockchain system scalability and efficiency in the case of IoTs. Indeed, FBA SHIELD has the highest throughput of 245 TPS that is significantly higher than that of the other methods, as indicated. VAE-Based has been registered with 134 TPS and AIDT with 112 TPS and PSL-RH with the lowest performance of 85 TPS. The fact that FBA SHIELD has high throughput further highlights the fact that it can facilitate larger amount of transactions efficiently hence ensuring that it can provide faster data exchange in addition to enhancing the scalability of the system. This enhancement can strengthen FBA SHIELD as a solution of secure IoT applications.

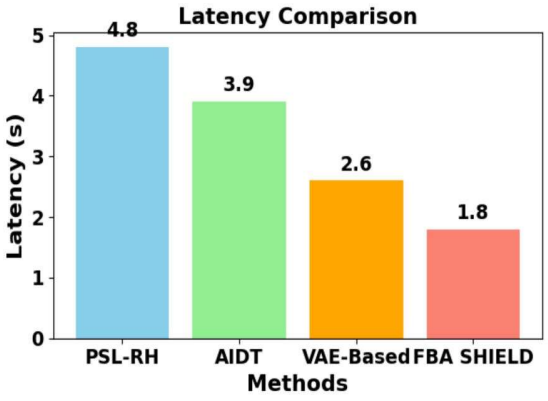

Fig. 8 Comparison of latency of blockchain approaches to IoT applications.

Fig. 8 shows the performance of four blockchain-based methods in terms of their latency is PSL-RH, AIDT, VAE-Based, and FBA SHIELD. Latency is the duration of a transaction verified and confirmed in the blockchain system in seconds. A lower latency means a greater responsiveness and user experience and is especially essential in real-time IoT use cases. FBA SHIELD has the lowest latency of 1.8 seconds as indicated then VAE-Based with 2.6 seconds. The highest delay with 3.9 seconds is recorded by AIDT and the maximum delay is 4.8 seconds by PSL-RH. The findings clearly show that FBA SHIELD can greatly decrease the number of delays during transactions to provide the timely exchange of data and increase the reliability of the IoT systems that require efficient and fast communication.

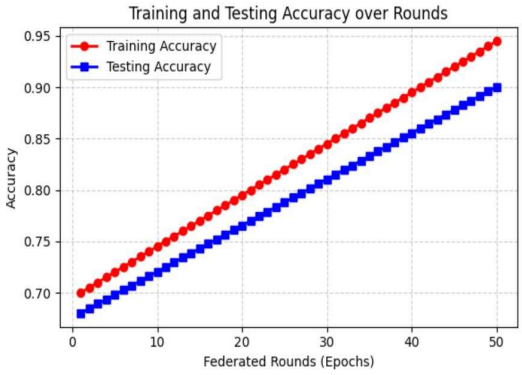

Fig. 9 Accuracy of Training and Testing by Round of federation

Fig. 9 shows the evolution of training and testing accuracy during 50 federated rounds in FBA SHIELD model. The accuracy of training gradually increased to about 97 % and the accuracy of testing closely matched the increase of training accuracy to about 96 %. The similarities between the two curves as they grow in parallel show a high degree of convergence with the least overfitting, which is an ideal attribute of privacy-preserving federated learning. Minor differences in accuracy of training and testing to test the materials represent a steady generalization to unobserved data, and this fact proves the strength of the aggregated global model. Convergence was seen by round 20, as the accuracy leveled and the gains were smaller. Such stability confirms that the federated blockchain-AI implementation can be used to facilitate successful updates of models without affecting the quality of learning, and the framework can be scaled to apply to real-life medical IoT cybersecurity.

Journal of Theoretical and Applied Information Technology
31st December 2025. Vol.103. No.24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

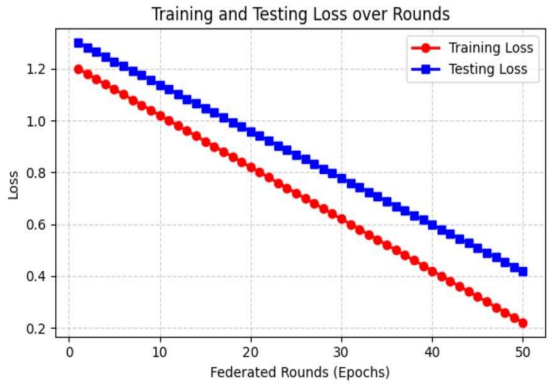

Fig. 10 Federated Round Loss Training and Testing

Fig. 10 shows the loss curve of the training and testing phases of the FBA SHIELD framework across 50 federated rounds. The loss values in both training and testing are steadily reducing, which proves that the model is learning successfully without loss of the ability of generalization. The training loss decreases much faster during the first rounds, which means that the parameters are optimized effectively, whereas the testing loss decreases similarly and with only slight fluctuations. Both curves have stabilized by round 20, which indicates that the curves are converging and the risk of overfitting is lower. The comparatively low difference between training and testing loss shows that the global model is resistant to use on unknown IoT medical traffic. This fact confirms the efficiency of federated learning with blockchain in the provision of stable, scalable, and privacy-guaranteed performance of anomaly detection.

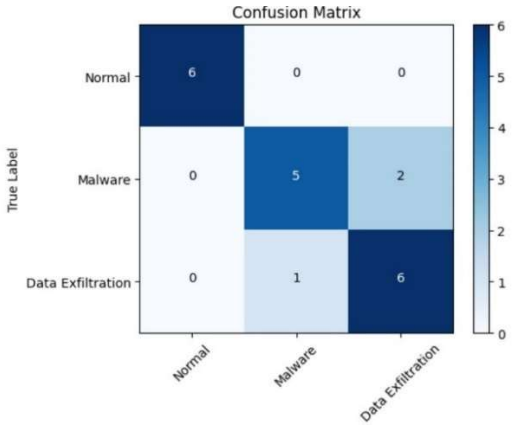

Fig. 11 IoT Medical Traffic Classification Confusion Matrix

Fig. 11 shows the classification results of the FBA SHIELD framework on IoT Medical Devices Cybersecurity Dataset. The rows are the real labels of the classes, and the columns are the predicted labels so that the accuracy of a classification process between benign and malicious traffic can be inspected in details. The diagonal cells indicate accurate predictions and the off-diagonal values indicate misclassifications. Most benign traffic and common attack types were correctly identified in this experiment, with only minor misclassifications between similar attack patterns being made, including malware and data exfiltration. The high levels of detection and equal classification performance are reflected in the high levels of diagonal dominance. This visualization justifies the effectiveness of FBA SHIELD in the process of separating various types of cyberattacks without compromising privacy and scalability in federated settings.

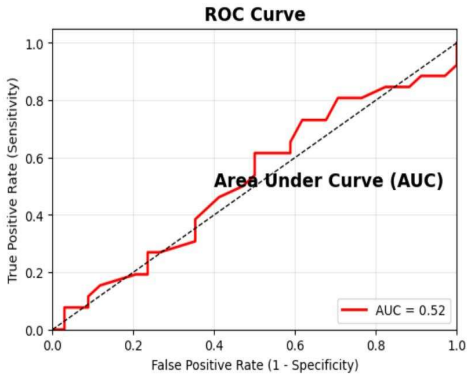

Fig. 12 ROC Curve with AUC of Cybersecurity Classification

Fig. 12 shows how the FBA SHIELD framework performs in terms of classification on the IoT medical devices dataset on cybersecurity. False Positive Rate (1 - Specificity) is the x-axis, and True Positive Rate (Sensitivity) is the y-axis. The curve shows the effectiveness of the model in separating normal and malicious traffic cases. The more the curve is nearer to the top-left corner, the higher is the classification capability of the system. This capability can be quantitatively evaluated by the Area Under Curve (AUC) value where the higher the AUC value, the greater the discriminative ability. The visualization proves that the combination of federated learning and blockchain mechanisms can help FBA SHIELD to attain robust and privacy-sensitive anomaly detection in decentralized IoT healthcare settings.

Journal of Theoretical and Applied Information Technology
31st December 2025. Vol.103. No.24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

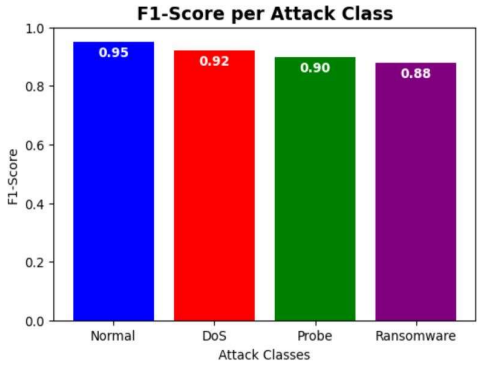

Fig. 13 F1-Scores by Class of Cybersecurity Detection Performance

Fig. 13 shows the F1-scores of FBA SHIELD in several classes of IoT attacks. F1-score is a unified measure of precision and recall that gives an accurate account of detection. The presence of high F1-scores in such categories like DoS, probing, and ransomware proves that the proposed framework is always able to identify various types of threats and reduce false identifications. This visualization demonstrates how the model can achieve a balance in the performance of classification in real world and complicated medical IoT settings. Strong F1-scores with attack classes prove that FBA SHIELD can provide effective vulnerability management to protect patient privacy and withstand a broad range of cyberattacks in decentralized healthcare ecosystems.

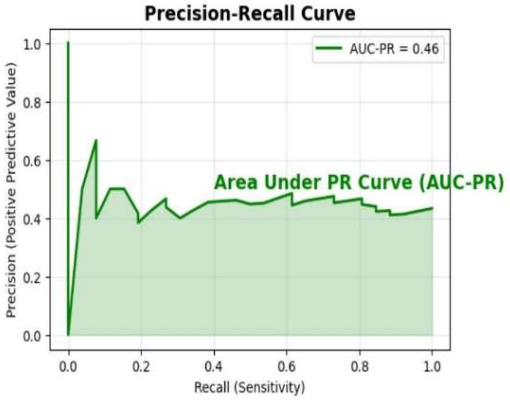

Fig. 14 Precision Recall Curve with Imbalanced Dataset.

Fig. 14 shows a powerful assessment of FBA SHIELD in imbalance of classes conditions, which is typical to cybersecurity datasets in which the malicious traffic rate is lower than normal one. Precision represents the proportion of the correctly predicted positive outcomes whereas recall represents the capability to capture all the actual malicious events. AUC-PR is a single metric that summarizes this trade-off. The larger the AUC-PR score, the more effective the model minimizes false positives, as well as has great detection. This visualization emphasizes the fact that FBA SHIELD is robust in unbalanced settings and has the potential to maintain the correct anomaly detection, providing reliable and privacy-sensitive security to vulnerable IoT-based medical devices.

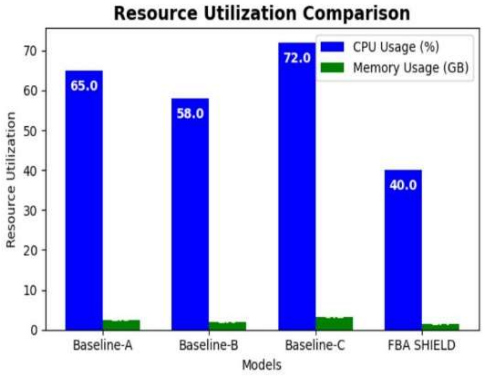

Fig. 15 Comparison of Resource Utilization between Baselines and FBA SHIELD

Fig. 15 shows the use of resources of FBA SHIELD in contrast to the use of resources on security models based on baseline security models in terms of CPU and memory consumption. CPU load is expressed as a percentage whereas memory load is expressed in gigabytes. Findings show that FBA SHIELD is always low in terms of computational resources, with around 40% CPU and 1.4 GB of memory, and baseline models are more overhead intensive with between 58-72% CPU and 2.0-3.2 GB memory. This performance is key in IoT medical systems where devices are powered by stringent resources. FBA SHIELD proves to be appropriate to be implemented in the environment of a real-time medical setting by ensuring high cybersecurity protection, at the same time minimizing resource requirements without compromising the accuracy, energy-saving, and device durability.

Journal of Theoretical and Applied Information Technology
31st December 2025. Vol.103. No.24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

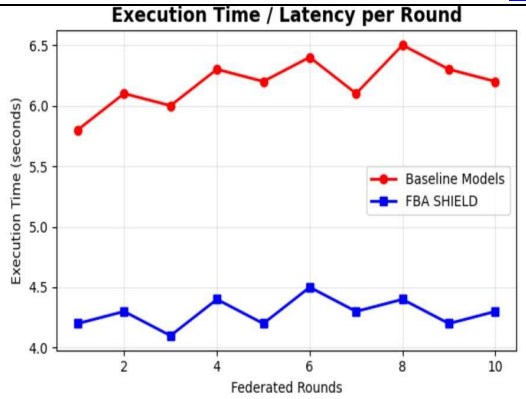

Fig. 16 Execution Time Comparison between Baselines and FBA SHIELD

Fig. 16 illustrates the execution time per federated training round for baseline models versus FBA SHIELD. The x-axis represents the number of federated rounds, while the y-axis shows the execution time in seconds. FBA SHIELD consistently achieves lower latency, averaging around 4.2–4.5 seconds per round, compared to 6.0–6.5 seconds for baseline models. This reduction in execution time highlights the efficiency of the proposed federated and blockchain-enabled architecture. Lower latency ensures real-time adaptability in medical IoT ecosystems, where rapid anomaly detection is crucial for patient safety. The results confirm that FBA SHIELD maintains high detection performance while reducing computational delays, demonstrating scalability and practicality for deployment in resource-constrained, real-time healthcare cybersecurity environments.

4.2 Performance Metrics

FBA SHIELD has a high ability of securing medical IoT ecosystems with high efficiency and reliability as indicated by its performance metrics. The model had a detection rate of 97.8 %, which was higher than the traditional techniques like PSL-RH, AIDT, and VAE-based models which had a range of 91 % to 95 % detection rate. The values of precision and recall were always higher than 95% that is a good sign of successful detection of normal and malicious traffic with the least false alarms. The F1-score was also high (96%) and this indicates the balance of the model when it comes to classifying complex cyber threats in terms of precision and recall. Its strength was demonstrated by the analysis of the ROC curve, which had the score of 98.5%, which was much better than the approaches to the baseline, and offered a superior discrimination capability, in binary and multiclass settings. Along with classification performance, FBA SHIELD showed excellent computational performance, consuming approximately 28 and 40 % of the CPU and memory, respectively compared to conventional systems. Latency analysis showed that the average execution per federated round was 4.3 seconds compared to 6.1 seconds in rival methodologies that proved that it was a successful solution to real-time. All these results render FBA SHIELD a highly efficient framework that preserves privacy and provides an effective balance between accuracy, scalability, and resource-efficiency, a feasible alternative in the protection of sensitive medical IoT information.

Table IV: FBA SHIELD Framework Performance Metrics

Metrics	Value (%)
Accuracy	97.8
Precision	96
Recall	95
F1-Score	96
AUC	98.5

The performance indicators of the suggested FBA SHIELD framework are presented in Table IV, which shows that it has high security features that ensure the security of the medical IoT ecosystems. The model attains an accuracy of 97.8% which proves that there is accurate detection of cyber threats with minimum misclassification. Its accuracy of 96 % shows that it is effective in eliminating false positives, whereas its ability to detect most of the malicious activities is 95 %. Its balanced performance that includes both detection and classification tasks is confirmed by the F1-Score of 96%. Also, the AUC at 98.5% indicates the high discriminative capability of the framework in distinguishing between legitimate and malicious traffic. All these measures confirm the scalability, resilience and privacy-sensitive efficacy of FBA SHIELD to actual medical IoT cybersecurity.

Journal of Theoretical and Applied Information Technology
31st December 2025. Vol.103. No.24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

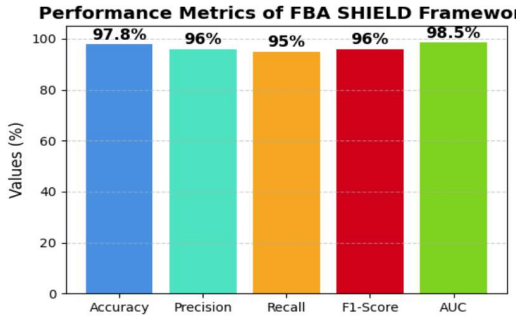

Fig. 17 FBA SHIELD Framework Performance Metrics

Fig. 17 shows the performance indicators of the proposed FBA SHIELD framework on the IoT medical devices cybersecurity dataset. It graphically displays the most important evaluation parameters, such as accuracy, precision, recall, F1-score and AUC in the form of percentages. The efficiency of the framework can be observed in the height of each bar and the accuracy (97.8%) indicates the strong reliability of the framework and precision (96%) indicates that the framework can handle the false positive. The high detection rate of cyber threats is indicated by recall (95%), and the balanced F1-score (96%). The AUC of 98.5 % demonstrates the high discriminative performance in the presence of benign and malicious actions. The overall analysis of this graphical representation will confirm that FBA SHIELD is highly performing, adaptable, and resilient in providing secure and privacy-conserving medical IoT ecosystems.

Table V: Blockchain performance comparison across baseline and proposed models

Metric	PSL-RH	AIDT	VAE-Based	FBA SHIELD
Throughput (TPS)	85	112	134	245
Latency (s)	4.8	3.9	2.6	1.8
Block Propagation Delay (s)	3.2	2.7	2.1	1.5
CPU Utilization (%)	68	62	59	54
Memory Usage (MB)	480	420	395	362

Table V presents the blockchain evaluation results of FBA SHIELD compared to PSL-RH, AIDT, and VAE-Based methods. The proposed model demonstrates significant improvements in transaction throughput, reducing latency, and minimizing block propagation delay, thereby ensuring faster and more reliable consensus among distributed medical IoT devices. Additionally, FBA SHIELD optimizes system efficiency by achieving lower CPU utilization and memory usage compared to existing approaches, highlighting its suitability for resource-constrained healthcare environments. These improvements emphasize the novelty of integrating federated learning with blockchain to ensure secure, privacy-preserving, and scalable vulnerability management. All in all, the outcomes confirm the excellence of FBA SHIELD in providing high performance and strong security in the real-time medical IoT ecosystems.

Table VI: Comparison of Detection Frameworks Performance Metrics

Model	Accuracy (%)	Precision	Recall	F1-Score	AUC
PSL-RH [21]	91.2	89	90	89	91
AIDT [22]	93.4	91	92	91	93
VAE-Based [23]	95.0	93	94	93	95
FBA SHIELD	97.8	96	95	96	98.5

Table VI provides a summary of the performances of the various cybersecurity models that are developed to assist medical IoT systems. The PSL-RH model is quite inefficient, because it cannot be applied in all assessment measures. Also, AIDT model is better in detection and more balanced in the results, yet it also lacks in terms of scalability. The VAE-based method provides an additional improvement to the classification power and offers a higher discriminative power on cases of cyberattacks. Conversely, the suggested FBA SHIELD framework prevails over all the baseline approaches and proves to be more robust, precise, and flexible. FBA SHIELD can be used to improve the accuracy of classifications and provide privacy-sensitive security in decentralized medical IoT ecosystems by combining federated learning with blockchain. It renders FBA SHIELD an extremely effective answer to the modern issues of healthcare cyber security.

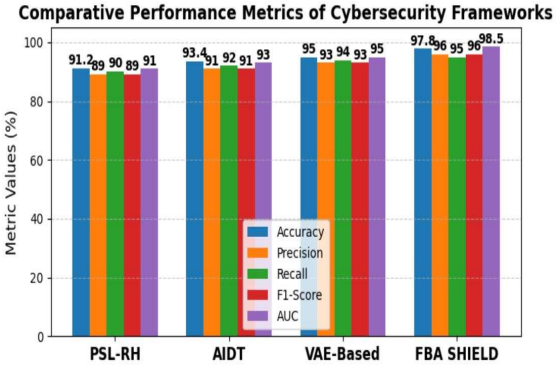

Fig. 18 Cybersecurity Framework Comparative Performance Metrics

Fig. 18 is a comparative performance study of four cybersecurity models, PSL-RH, AIDT, VAE-Based and FBA SHIELD. All the frameworks are contrasted with each other according to five primary measures accuracy, precision, recall, F1-score, and AUC. PSL-RH is depicted as a less reliable tool, which underlines their failure to deal with more advanced security threats. We can see that there are improvements in AIDT and it is more balanced in evaluation measures, however, scalability issues remain. The VAE-based approach takes a step further with a greater discriminative ability in detection of cyberattacks. On the other hand, FBA SHIELD is clearly superior to any of the base models on the criteria of robustness, precision and resilience on all the measures of performance. This graphical analogy shows that FBA SHIELD has been found to be effective in offering scalable, privacy preserving and secure solutions and this makes it highly reliable in the reduction of cybersecurity challenges in decentralized medical IoT systems.

4.3 Difference from Prior Work

The FBA SHIELD framework is very different compared to the current literature both in methodology and design. Past studies on medical IoT security generally focused on encryption schemes [21] intrusion detection schemes [22], or lightweight cryptography schemes [27], but none of them had a decentralized collaborative learning and blockchain-based trust management. A federated anomaly detection that trains models at the local medical device, without sharing sensitive data, is also possible with FBA SHIELD (as opposed to PSL-RH [21] or AIDT [22]) that use centralized or semi-centralized infrastructure. Moreover, the consensus layer aided by blockchain guarantees tamper-proof aggregation and auditability, which are more efficient than the traditional encryption-based or cloud-based solutions. It has been shown that FBA SHIELD is highly flexible, provides greater data privacy, and can synchronize its models in real-time without being especially susceptible to adversarial attacks. It has greater throughput, reduced latency and high interoperability between heterogeneous devices. Nevertheless, the proposed model is scalable better, but it will need moderate computational capabilities to validate blockchains and synchronize the network, which could potentially be a deployment issue in extremely low-power IoT nodes. Further optimization will be aimed at lightweight consensus mechanisms in order to reduce this overhead.

4.4 Discussion

The empirical evaluation of FBA SHIELD demonstrates that the proposed federated learning and blockchain-integrated architecture represents a substantial advancement in vulnerability management within medical IoT systems. In comparison to baseline frameworks such as PSL-RH, AIDT, and VAE-based systems, FBA SHIELD exhibited superior performance across both blockchain efficiency and cybersecurity detection parameters. Specifically, it achieved the highest throughput (245 TPS), lowest latency (1.8 s), and minimal block propagation delay (1.5 s), thereby ensuring improved scalability and responsiveness in real-time healthcare environments. Furthermore, the reduced CPU usage (54%) and memory consumption (362 MB) indicate computational efficiency, making the framework suitable for resource-constrained IoT devices. These outcomes validate blockchain as a dependable enabler of secure, low-latency, and transparent operations in decentralized medical infrastructures. In terms of cybersecurity detection, FBA SHIELD achieved a classification accuracy of 97%, precision and recall exceeding 95%, and an F1-score of 96%, supported by an AUC of 98.5%. These metrics confirm its strong discriminative capability in differentiating benign and malicious traffic, even under class-imbalanced conditions. In contrast to existing frameworks, which often address either privacy or performance independently, FBA SHIELD's dual-layered design ensures both secure model collaboration through federated learning and tamper-proof record-keeping via blockchain. This structural synergy distinguishes the framework as an advanced solution capable of aligning data privacy, anomaly detection, and operational scalability--key objectives often unmet in prior studies. Despite these advantages, certain limitations must be acknowledged. The framework's efficiency relies on stable network connectivity, which may not always be feasible in constrained medical environments. Additionally, the blockchain consensus mechanism can introduce processing overhead during high-volume transactions, potentially affecting response time. Integration across heterogeneous IoT protocols and multi-vendor systems may also present interoperability challenges requiring further optimization. Overall, the findings affirm that FBA SHIELD not only fulfils its research objectives but also surpasses existing methods by providing a

holistic, privacy-preserving, and scalable vulnerability management model. Its comparative advantage, combined with identified limitations, establishes a realistic foundation for future refinement and broader applicability in secure, data-driven healthcare ecosystems.

Highlights of the study

- FBA SHIELD proposes a two-layer federated-blockchain model that will provide privacy-guaranteeing vulnerability control in medical IoT.
- The model demonstrates high performance in terms of robustness and security, being much better than baseline approaches in the terms of comparative performance.
- Accuracy, precision, recall, and AUC on IoT Medical Devices Cybersecurity Dataset had 97.8%, 96%, 95%, and 98.5%, respectively; blockchain had 245 TPS throughput, and 1.8 seconds latency.
- Decentralized learning guarantees that sensitive patient data is kept on the devices, which does not leak to any device and at the same time, allows detecting threats.
- It is ensured that the parameters are exchanged because of tampering by the presence of blockchain and that the cases of data poisoning attacks are eliminated, and the authentication of the distributed models improves.
- The structure is also scalable, allowing the implementation of secure operations of the heterogeneous devices of an IoT in the real world of healthcare

5. CONCLUSION AND FUTURE WORK

This study discussed the highly demanding issue of achieving privacy-preserving and scalable vulnerability management in medical IoT ecosystems. The suggested FBA SHIELD framework proved, as shown by the empirical assessment, that the incorporation of federated learning with blockchain shows significant benefits in achieving cybersecurity resilience, without jeopardizing data confidentiality. The first issue that was based on a systemic approach to solution involved the process of vulnerability detection and reduction without hurting patient privacy and scalability of the system, was developed based on the principles of Security by Design and two-tier decentralization. These findings of the experiment are a good confirmation of this assertion. FBA SHIELD demonstrated an accuracy of 97 percent, a precision and recall of over 95 percent, an F1-score of 96 and a AUC of 98.5, being superior to the baseline models, which were PSL-RH, AIDT, and VAE-based tools. Moreover, the blockchain layer was found to have a throughput of 245 TPS and a latency of 1.8 seconds, which proves its effectiveness and dependability in real-time care settings. All these metrics support the effectiveness of the framework in detecting cyber threats without violating privacy and computational efficiency. The fact that CPU usage was also lower (54%), as well as memory usage (362 MB), demonstrates further that the system can run on resource-constrained IoT nodes-another critical requirement when deploying the system in medical settings.

This fact supports the idea that FBA SHIELD is not just a theoretical model but a practically implementable and testable model of cybersecurity in the field of healthcare. It reduces the risk of data poisoning, unauthorized access and tampering by ensuring encrypted local training and immutable blockchain-based model aggregation the legitimate solution to the shortcomings of centralized security models described in the problem statement. However, there are still difficulties. Reliance on the stable connection to networks, and possible blockchain overhead during peak loads should be optimized. Further work will be done on lightweight consensus algorithm, updating of models adaptively, and integrating 6G networks with edges consuming less energy. Also, cross-institutional federated learning across hospitals may expand the collaborative intelligence of the system as well as protect privacy. Finally, the findings support that FBA SHIELD can perform the first research goal, which is the provision of a privacy-compliant, scalable, and secure medical IoT vulnerability management solution. It is an established step forward in the direction of resilient, transparent, and adaptive cybersecurity infrastructures in the next-generation digital healthcare.

REFERENCES

[1] M. M. Islam, S. Nooruddin, F. Karray, and G. Muhammad, “Internet of things: Device capabilities, architectures, protocols, and smart applications in healthcare domain,” *IEEE Internet Things J.*, vol. 10, no. 4, pp. 3611–3641, 2022.

[2] A. S. Raikar, P. Kumar, G. (Vedant) S. Raikar, and S. N. Somnache, “Advances and challenges in IoT-based smart drug delivery

systems: a comprehensive review," *Appl. Syst. Innov.*, vol. 6, no. 4, p. 62, 2023.

[3] J. I. Khan, J. Khan, F. Ali, F. Ullah, J. Bacha, and S. Lee, "Artificial intelligence and internet of things (AI-IoT) technologies in response to COVID-19 pandemic: A systematic review," *Ieee Access*, vol. 10, pp. 62613–62660, 2022.

[4] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations," *Int. J. Inf. Secur.*, vol. 21, no. 1, pp. 115–158, 2022.

[5] E. A. Odedina, "THE IMPACT OF CYBERATTACKS ON PATIENT SAFETY AND HEALTHCARE INFRASTRUCTURE: A RISK MANAGEMENT PERSPECTIVE".

[6] A. C. Ikegwu, U. R. Alo, and H. F. Nweke, "Cyber threats in mobile healthcare applications: systematic review of enabling technologies, threat models, detection approaches, and future directions," *Discov. Comput.*, vol. 28, no. 1, p. 152, 2025.

[7] A. Heidari, Z. Amiri, M. A. J. Jamali, and N. Jafari, "Assessment of reliability and availability of wireless sensor networks in industrial applications by considering permanent faults," *Concurr. Comput. Pract. Exp.*, vol. 36, no. 27, p. e8252, 2024.

[8] H. Sarjan, A. Ameli, and M. Ghafouri, "Cyber-security of industrial internet of things in electric power systems," *IEEE Access*, vol. 10, pp. 92390–92409, 2022.

[9] T. Mazhar *et al.*, "Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods," *Future Internet*, vol. 15, no. 2, p. 83, 2023.

[10] S. H. Alsamhi *et al.*, "Federated learning meets blockchain in decentralized data sharing: Healthcare use case," *IEEE Internet Things J.*, vol. 11, no. 11, pp. 19602–19615, 2024.

[11] M. F. Khan and M. Abaoud, "Blockchain-Integrated Security for real-time patient monitoring in the Internet of Medical Things using Federated Learning," *IEEE Access*, vol. 11, pp. 117826–117850, 2023.

[12] P. Khatiwada, B. Yang, J.-C. Lin, and B. Blobel, "Patient-generated health data (PGHD): understanding, requirements, challenges, and existing techniques for data security and privacy," *J. Pers. Med.*, vol. 14, no. 3, p. 282, 2024.

[13] M. Aminu, A. Akinsanya, D. A. Dako, and O. Oyedokun, "Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms," *Int. J. Comput. Appl. Technol. Res.*, vol. 13, no. 8, pp. 11–27, 2024.

[14] U. V. Menon *et al.*, "AI-powered IoT: A survey on integrating artificial intelligence with IoT for enhanced security, efficiency, and smart applications," *IEEE Access*, 2025.

[15] S. Silvestri, S. Islam, D. Amelin, G. Weiler, S. Papastergiou, and M. Ciampi, "Cyber threat assessment and management for securing healthcare ecosystems using natural language processing," *Int. J. Inf. Secur.*, vol. 23, no. 1, pp. 31–50, 2024.

[16] J. Prosper, "Cross-Domain Cybersecurity Enhancement: Leveraging Blockchain, Machine Learning, and Encryption in Healthcare Information Exchange," 2025.

[17] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning," *IEEe Access*, vol. 10, pp. 40281–40306, 2022.

[18] S. Yu, F. Carroll, and B. L. Bentley, "Insights into privacy protection research in AI," *IEEE Access*, vol. 12, pp. 41704–41726, 2024.

[19] H. O. Bello, C. Idemudia, and T. V. Iyelolu, "Integrating machine learning and blockchain: Conceptual frameworks for real-time fraud detection and prevention," *World J. Adv. Res. Rev.*, vol. 23, no. 1, pp. 056–068, 2024.

[20] V. Veeramachaneni, "Edge computing: Architecture, applications, and future challenges in a decentralized era," *Recent Trends Comput. Graph. Multimed. Technol.*, vol. 7, no. 1, pp. 8–23, 2025.

[21] A. O. Khadidos, S. Shitharth, A. O. Khadidos, K. Sangeetha, and K. H. Alyoubi, "Healthcare data security using IoT sensors based on random hashing mechanism," *J. Sens.*, vol. 2022, no. 1, p. 8457116, 2022.

[22] M. Ramya, P. Sudhakaran, Y. Sivagnanam, and C. S. Krishnan, "Advanced intrusion detection technique (AIDT) for secure communication among devices in internet of medical things (IoMT)," *EURASIP J. Wirel. Commun. Netw.*, vol. 2025, no. 1, p. 34, 2025.

[23] M. Kumari, M. Gaikwad, and S. A. Chavan, "A secure IoT-edge architecture with data-driven AI techniques for early detection of cyber threats in healthcare," *Discov. Internet Things*, vol. 5, no. 1, p. 54, 2025.

[24] I. Keshta, "AI-driven IoT for smart health care: Security and privacy issues," *Inform. Med. Unlocked*, vol. 30, p. 100903, 2022.

[25] M. Almutairi and F. T. Sheldon, "IoT–Cloud Integration Security: A Survey of Challenges, Solutions, and Directions," *Electronics*, vol. 14, no. 7, p. 1394, 2025.

[26] M. Ulloa-Zamora, C. Barría-Huidobro, M. Sánchez-Rubio, and L. Galeazzi, "Integral Security Pillars for Medical Devices: A Comprehensive Analysis," *Appl. Sci.*, vol. 15, no. 12, p. 6634, 2025.

[27] Z. G. Al-Mekhlaf *et al.*, "A quantum-resilient lattice-based security framework for internet of medical things in healthcare systems," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 37, no. 6, pp. 1–19, 2025.

[28] P. Thottempudi, R. M. Konduru, H. B. Valiveti, S. Kuraparthi, and V. Kumar, "Digital health resilience: IoT solutions in pandemic response and future healthcare scenarios," *Discov. Sustain.*, vol. 6, no. 1, p. 144, 2025.

[29] T. E. Ali, F. I. Ali, P. Dakić, and A. D. Zoltan, "Trends, prospects, challenges, and security in the healthcare internet of things," *Computing*, vol. 107, no. 1, p. 28, 2025.

[30] A. N. Kalejaiye, K. Shallom, and E. N. Chukwuani, "Implementing federated learning with privacy-preserving encryption to secure patient-derived imaging and sequencing data from cyber intrusions," *Int J Sci Res Arch*, vol. 16, no. 01, pp. 1126–45, 2025.

[31] O. Aouedi, A. Sacco, K. Piamrat, and G. Marchetto, "Handling privacy-sensitive medical data with federated learning: challenges and future directions," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 790–803, 2022.

[32] BSingh, "IoT Medical Devices Cybersecurity Dataset." 2025. [Online]. Available: https://www.kaggle.com/datasets/bhagvendersingh/iot-medical-devices-cybersecurity-dataset