IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.141281

MedGuard Edge: Intelligent Cyber Defense for Healthcare IoT Devices

Vasavi P[1], Mrs Visalini S[2], Navya M[3], Navyashree N[4], Sanjana S[5]

Department of Information Science and Engineering, The Oxford College of Engineering,

Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India[1-5]

Abstract: MedGuard Edge is a decentralized healthcare IoT system that ensures continuous and secure patient monitoring while solving the fundamental security and privacy concerns of traditional centralized systems. The smart wearable hand band includes sensors for temperature, oxygen saturation (SpO_2), heart rate (BPM), and humidity, which process crucial biomedical data. These data are encrypted and transferred to the MedGuard server via a Node MCU module for threat analysis, anomaly identification, and decision-making, with the user receiving emergency notifications. At its core, Clustered Federated Learning allows for local model training on clustered devices without exchanging raw patient data, hence ensuring privacy. Blockchain technology secures model updates via tamper-proof validation, ensuring data integrity. Real-time anomaly detection monitors devices and data for anomalies, while self-healing features isolate or recover compromised nodes to ensure system stability. A real-time dashboard displays graphical views of patient data, alerts, device health, and blockchain logs, allowing healthcare administrators to monitor and respond more efficiently.

Keywords: Blockchain, Clustered Federated Learning, Internet of Things (IoT), Healthcare Security, Anomaly Detection, and Self-Healing Systems.

I. INTRODUCTION

MedGuard Edge is a cutting-edge next-generation digital healthcare platform that combines Clustered Blockchain and CFL improve the security, scalability, and effectiveness of IoT networks. IoT devices minimize data transmission and protect privacy by locally training models on their own datasets. sensitive health data, MedGuard Edge decentralizes data processing, in contrast to typical centralized healthcare systems that concentrate it in a single location. Instead of sending raw medical records over the network, the system simply shares encrypted model updates to preserve patient privacy.

Blockchain acts as the foundational technology for maintaining data security and integrity fostering transparency, with every transaction, model update, and access event immutably recorded on a distributed ledger that is resistant to tampering and fraud. The system includes real-time anomaly detection systems that track each device's activities in order to improve security. The system may automatically isolate the affected node and start recovery procedures if suspicious or malicious activity is found, ensuring consistent and reliable healthcare service delivery. Clustering of IoT devices within the CFL framework improves the scalability and efficiency of the learning process, allowing the system to successfully manage various IoT contexts. complex healthcare contexts. In addition, this clustering method improves energy usage and communication overhead, which is critical for medical devices with limited resources.

Together, these components provide a solid digital healthcare architecture that facilitates precise diagnosis, real-time patient monitoring, and compliance with strict data standards. MedGuard Edge opens the door to a secure, scalable, and intelligent healthcare IoT infrastructure suitable for the future of connected health by combining decentralized learning, blockchain-based security, and intelligent anomaly handling.

II. PROBLEM STATEMENT AND OBJECTIVE

Centralized IoT healthcare solutions are inherently vulnerable to system outages, unauthorized access, and breaches of patient confidentiality, which can undermine trust and compromise compliance with privacy laws.
The MedGuard Edge framework is designed to confront these risks by decentralizing data processing, employing devices clustered for federated learning so that sensitive medical information is locally safeguarded rather than consolidated on central servers. Blockchain technology underpins the verification of model updates, providing a transparent and immutable audit trail that ensures data accuracy and security throughout the healthcare network. Advanced self-healing mechanisms, combined with real-time anomaly detection, reinforce overall system resilience and facilitate rapid response to potential threats or network failures. By leveraging clustered device architectures, MedGuard Edge enhances both the

 This work is licensed under a Creative Commons Attribution 4.0 International License

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025
DOI: 10.17148/IJARCCE.2025.141281

efficiency and scalability of distributed learning, making it adaptable for growing healthcare infrastructures while upholding stringent data privacy standards and regional regulatory requirements.
Key objectives of MedGuard Edge:

- Preserve data privacy.
- Verify model updates in a transparent and safe manner with blockchain technology.
- Include self-healing and anomaly detection systems to increase network resilience.
- Enhance efficiency and scalability through device clustering.
- Verify compliance with relevant healthcare data privacy laws.

III. SCOPE

The MedGuard Edge system provides a complete and innovative solution designed to tackle the urgent issues that healthcare IoT environments face. By guaranteeing that sensitive patient The IoT devices process the data directly, this decentralized framework reduces the dangers connected with centralized data storage and transfer, improving data privacy. Data integrity and regulatory compliance are ensured by the incorporation of blockchain technology, which offers a transparent and unchangeable method for confirming model revisions. In order to sustain ongoing healthcare service delivery, the structure system's anomaly detection and self-healing features enhance network resilience by enabling real-time reaction to security threats and operational errors. MedGuard Edge greatly increases scalability and energy efficiency by using device clustering within Clustered Federated Learning, which enables it to adapt to the dynamic and frequently resource-constrained healthcare settings. In order to provide wide compatibility and future-proof the framework, the scope also includes supporting a range of clinical data sources and IoT devices for healthcare accommodating growing medical technology. In decentralized health systems, the framework's flexible design promotes cross-institutional cooperation and cloud interoperability. It also makes it easier to include cutting-edge AI-based prediction technologies, allowing physicians to offer proactive care and timely diagnoses. All things considered, MedGuard Edge is a prime example of both a strong security solution and an intelligent, scalable, and compliant infrastructure that can adapt to changing healthcare needs and technology breakthroughs. MedGuard Edge is positioned to revolutionize digital healthcare by enabling creative and efficient healthcare delivery through the deployment of a safe and privacy-focused IoT network.

IV. LITERATURE REVIEW

[1] Alami et al. The system may identify rogue IoT devices without transmitting raw data by utilizing Federated Learning in conjunction with a permissioned blockchain, resulting in low false positives and high detection accuracy.

[2] Alsamhi et al. proposed an FL–Blockchain architecture for healthcare, where patient data stays local and smart contracts manage secure model exchange. Their multi-hospital simulations show improved privacy and auditability, but highlight overhead on resource-limited devices.

[3] Ying et al. introduced BIT-FL, an incentivized FL system that rewards clients for high-quality model updates using blockchain smart contracts. Experiments show improved accuracy and participation, although incentive mechanisms may introduce new vulnerabilities.

[4] Yuan et al. addressed scalability with a layered and sharded blockchain that parallelizes model update verification. Their approach significantly improves throughput and reduces validation latency in large FL networks.

[5] Lin et al. proposed a time-efficient blockchain-based FL workflow that prioritizes low-latency clients to speed up convergence. While effective for real-time IoT, this method raises fairness concerns for slower devices.

[6] Huang et al. designed FL chain, a lightweight FL–Blockchain system optimized for low computational and communication overhead. Despite its simplicity, it maintains tamper-evidence and integrity, making it suitable for IoT healthcare devices.

[7] Ahmed et al. presented a blockchain-secured FL framework for classifying AIoMT devices. Their system supports decentralized model sharing while preserving provenance, validated through device datasets and simulated hospital environments.

[8] Dong et al. proposed a blockchain-based mechanism to defend against poisoning attacks in FL by logging updates and detecting anomalies. The outcomes show enhanced resilience and successful client segregation.

DOI: 10.17148/IJARCCE.2025.141281

[9] Yang & Xing integrated homomorphic encryption with blockchain-managed FL to ensure encrypted model updates throughout aggregation. Their approach enhances privacy for multi-hospital collaboration despite higher computational costs.

[10] Issa et al. provided a comprehensive survey of blockchain-enabled FL for IoT, outlining architectures, threats, and cryptographic strategies. They identify research gaps such as dynamic clustering and real-time anomaly handling, motivating more adaptive FL systems.

4.1 Gaps or Areas for Improvement

Despite considerable advancements in the fusion of federated learning with blockchain for safe and expandable Internet of Things healthcare systems healthcare IoT environments, several gaps and limitations remain unaddressed in existing research. A notable constraint is the lack of models for Clustered Federated Learning (CFL). Large, diverse healthcare IoT applications have limited scalability because to the single-layer, flat structure of most existing FL systems, which also results in high communication costs. CFL, which groups devices into smaller and more manageable clusters to improve training efficiency, remains significantly underexplored in medical applications. Another critical gap is the absence of self-healing capabilities and real-time threat detection. While privacy-preservation has been widely emphasized, many existing solutions fail to incorporate autonomous intrusion detection mechanisms or automatic fault-recovery features. These functionalities are essential in healthcare environments, where continuous monitoring and uninterrupted device operation are crucial for patient safety. In addition, current blockchain-FL systems often lack healthcare-specific optimization. Many frameworks are designed for generic IoT scenarios and do not consider medical requirements such as ultra-low latency, device heterogeneity, strict reliability constraints, and patient-safety-driven protocols. Tailored models that address these domain-specific needs are still limited.

Furthermore, many studies continue to rely on centralized or cloud-based storage for logs and system metadata, creating vulnerabilities despite using blockchain. Fully decentralized storage solutions such as IPFS, which enhance data availability and integrity, are still not widely adopted. Finally, energy efficiency and scalability pose significant challenges. Healthcare IoT devices usually operate under tight power constraints, and heavy cryptographic operations or blockchain consensus mechanisms can overwhelm these devices. To enable scalable, sustainable systems, striking a balance between strong security and energy efficiency remains an open research problem.

V. SYSTEM ARCHITECTURE

The MedGuard Edge framework establishes a comprehensive, decentralized architecture designed to address the critical challenges faced by healthcare IoT systems, including data privacy, security, scalability, and resilient management. Fundamentally, important patient data including blood pressure, heart rate, temperature, and oxygen saturation are continuously gathered by wearable sensors and medical monitoring devices. These devices preprocess the data locally, cleaning, normalizing, and filtering it to maintain patient privacy and reduce data transmission burdens. Above this lies the Clustered Federated Learning (CFL) layer, which organizes IoT devices into logical clusters based on factors like device type, geographic location, or data similarity. A model for local machine learning is trained by every gadget, and the cluster head only receives model updates. These updates are combined by the cluster head to create a cluster-level model, which then adds to a global model that depicts the complete system.

This hierarchical training approach enhances model efficiency, significantly cuts down communication costs, and supports scalability far better than traditional flat federated or centralized methods. To ensure the authenticity Regarding the model's integrity updates, the system employs a blockchain layer where every update is validated and immutably recorded using smart contracts. A central authority is no longer necessary thanks to this decentralization, which also shields the system from malicious attacks or tampering that can jeopardize the accuracy of the model or the reliability of the data. Complementing blockchain is the Interplanetary File System (IPFS), used for decentralized storage of validated model updates, anomaly reports, and other critical system information. IPFS ensures fault tolerance, high availability, and rapid data retrieval, even if parts of the network fail, thereby reinforcing system robustness. A dedicated anomaly detection and self-healing layer continuously monitors network and device activities for abnormal patterns such as unauthorized access or malfunctioning nodes. When issues are detected, the system autonomously isolates compromised devices, initiates restorative actions like resets or reconfigurations, and reintegrates the devices once stability is achieved. This reduces downtime and enhances the network’s overall resilience. Finally, system administrators are supported by a user-friendly, web-based dashboard that provides real-time visualization of blockchain transactions, security threats, device performance, and mitigation efforts. This interface enables proactive management and transparent oversight, empowering administrators to maintain optimal system health and security.

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.141281

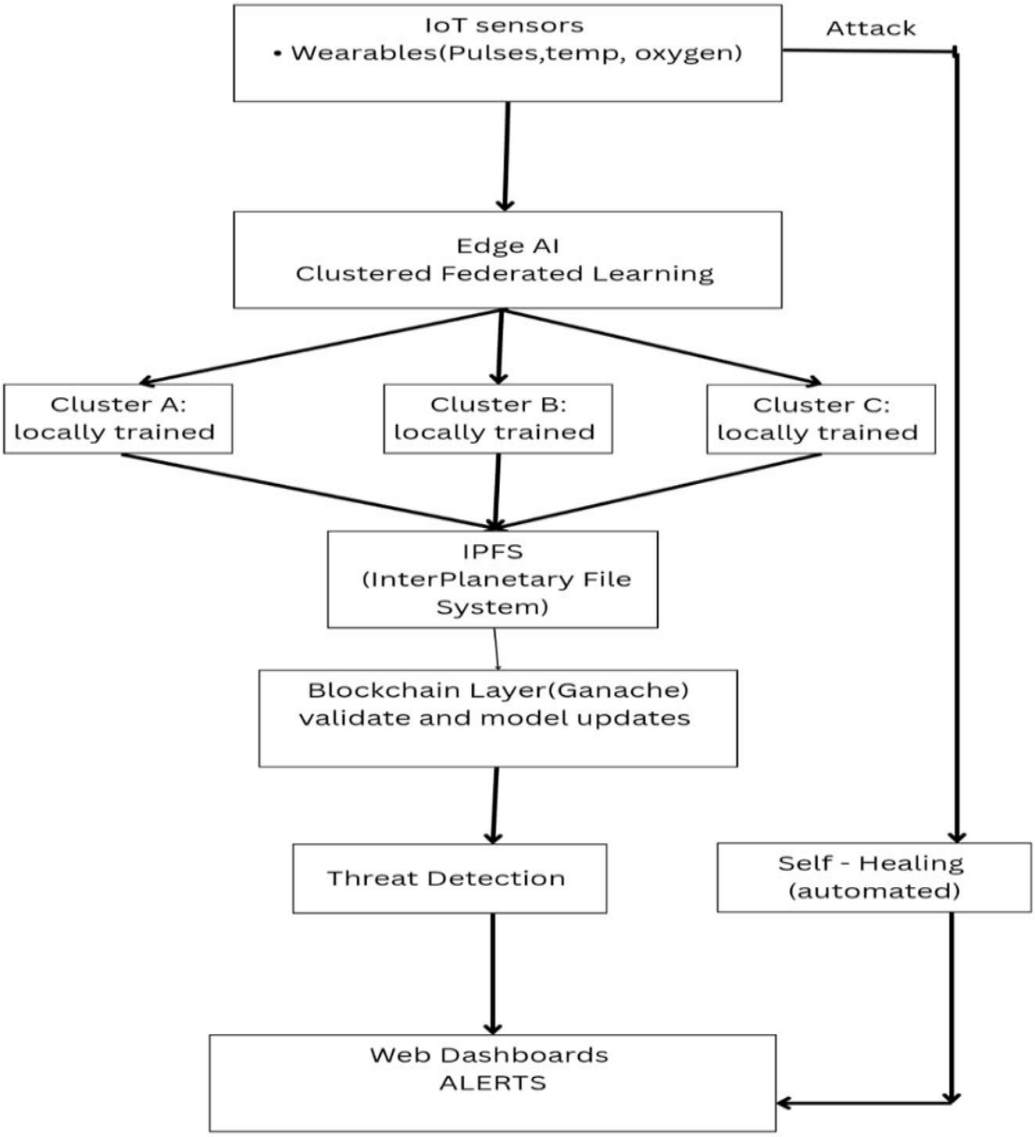

Figure 1: Complete system architecture showing integration of blockchain validation, clustered federated learning, IPFS storage, real-time monitoring dashboard

In summary, MedGuard Edge fuses hierarchical federated learning, blockchain-secured validations, decentralized fault-tolerant storage, intelligent anomaly detection with self-healing, and comprehensive real-time monitoring into a unified architecture. This design effectively addresses the pressing needs of healthcare IoT networks by safeguarding sensitive patient data, ensuring reliable system operation, and enabling scalable, adaptive intelligence for modern medical environments.

VI. METHODOLOGY

The MedGuard Edge system is constructed upon a multi-layered decentralized architecture that brings together blockchain verification, decentralized storage via IPFS, autonomous self-healing capabilities, and Clustered Federated Learning (CFL) to guarantee a secure, scalable, and privacy-preserving environment for healthcare IoT devices. This integrated model ensures the system's integrity, availability, and resilience even under adverse conditions.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.141281

6.1 IOT Data Gathering

The foundation lies in a network of IoT gadgets deployed within healthcare environments, including wearable sensors as well as patient monitoring devices. These devices continuously monitor crucial patient physiological information, such as blood pressure, heart rate, body temperature, and oxygen saturation pressure, and oxygen saturation. The information gathered is used to train and update localized models for machine learning, enabling accurate and timely patient health assessments.

6.2 Preprocessing Local Data

Each IoT device performs on-device preprocessing, which involves cleaning the collected data, normalizing it to a standard format, and handling missing or inconsistent values locally. By reducing pointless data transfer, this method lowers communication overhead while simultaneously increasing model training accuracy.

Timestamp	SpO_2	Pulse	Temp	Humi
19-11-2025 14:17	92.44	82	27	59
19-11-2025 14:17	100	85	27	59
19-11-2025 14:17	93.47	85	27	59
19-11-2025 14:17	93.29	89	27	59
19-11-2025 14:17	91.32	82	27	59

Table 1: Sample sensor log readings

6.3 Device Cluster Formation

To improve scalability and reduce latency, IoT gadgets are logically arranged into clusters according to standards such gadget type, data similarity, or geographic proximity. Under the direction of a cluster head who oversees local data gathering and model training within the group, each cluster functions somewhat independently. This clustered federated learning approach boosts bandwidth efficiency and accelerates convergence by localizing intensive communication.

Cluster	O_2	Pulse	Temp	Humi
1	92.84	88.12	27.00	59.00
2	87.17	76.38	24.99	55.03
3	93.20	72.80	27.00	59.00

Table 2: Cluster summary statistics

6.4 Training Local Models

Within each device cluster, individual IoT devices are used to directly train local machine learning models using their respective pre-processed datasets. Importantly, patient raw data remain secure on the devices. The models capture vital data patterns and insights unique to each patient's profile. After training, these devices transmit only model modifications to the cluster head for secure aggregation.

6.5 Global Model Integration and Cluster-Level Aggregation

In order to create cluster-level models that reflect localized learning outcomes, cluster chiefs gather local model updates from their devices. These cluster models are then forwarded to a global aggregator that fuses the aggregated updates into a comprehensive global model. This hierarchical aggregation technique significantly reduces overhead in communication while enhancing the general model's accuracy and generalizability across diverse healthcare populations.

6.6 Blockchain-Based Verification

All improvements to the model and cluster-level aggregations are recorded and validated in a blockchain ledger through the execution of smart contracts. The blockchain consensus mechanism ensures that every update is authentic, immutable, and traceable, thereby fostering transparency and trust among participating devices and stakeholders. This decentralized verification process prevents data tampering and increases overall system security.

6.7 IPFS-based decentralized storage

MedGuard Edge securely stores approved model updates, training logs, and anomaly detection data over IPFS. This decentralized storage solution guaranty's fault tolerance, high data availability, and redundancy by distributing data across multiple network nodes. Even if some nodes become inoperative, the system maintains continuous access to critical information, enhancing resilience.

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.141281

6.8 Identifying Anomalies and Preventing Intrusions

An anomaly detection module persistently monitors device activities, data flows, and network traffic to detect suspicious behaviours such as unauthorized access attempts, data breaches, or unusual communication patterns. Upon detecting anomalies, the system immediately triggers mitigation actions that can include limiting network access, isolate malicious nodes, or block hostile entities to avoid the propagation of attacks.

6.9 Threat Response, System Shutdown, and Safe File Recovery

MedGuard Edge has an automated shutdown response mechanism to prevent widespread compromise after repeated intrusion attempts. Every unauthorized or anomalous occurrence raises a threat counter. The system continuously tracks IP access patterns, CSV file requests, and strange data behaviours. The framework initiates a secure shutdown mode to stop further activity and stop data corruption when this counter reaches twenty consecutive violations. The blockchain-verified baseline file is then retrieved by the system from IPFS, guaranteeing the restoration of a secure, reliable dataset even in the event that an attacker targets numerous files. Data integrity is maintained, cascading failures are avoided, and the system is ready for a safe restart upon administrator verification, thanks to our secure recovery method.

Figure 2: Threat-Response Shutdown Triggered After Repeated Anomalies

6.10 Dashboard for Monitoring and Visualization

Healthcare administrators are provided with a comprehensive, web-based dashboard offering real-time monitoring and visualization of the system's operational and security status. This interface presents crucial metrics such as blockchain-verified transactions, network performance, device health indicators, and active security threats. The dashboard facilitates timely decision-making, early identification of possible dangers, and effective administration of the healthcare IoT infrastructure.

VII. IMPLEMENATION ENVIRONMENT

The recommended MedGuard Edge system's implementation environment combines hardware and software elements to allow for decentralized validation, intelligent analysis, and safe data collection. Data preprocessing, SHA-256-based authenticity validation, clustered supervised learning, identifying anomalies, and connection with chain and IPFS services are all supported by the system's primary programming language, Python. Solidity is used in blockchain smart contract implementation to safely store model modifications, IPFS hash values, and audit trails, guaranteeing transparency and defense against unwanted changes. Ganache is used to establish a localized Ethereum blockchain environment for the effective deployment and testing of smart contracts without actual gas expenses. Through JSON-RPC, Web3.py enables communication among the Python back and the blockchain, enabling immutable logging, hash storage, contract execution, and update verification. As the backend server, Flask manages network operations, IPFS uploads, anomaly warnings, federated training workflows, sensor data receipt, and immediate dashboard communication.

The Arduino Uno microcontroller, which is based on the ATmega328P and operates at 5V with a 16 MHz clock and has numerous analogue and digital input/output pins for sensor interfacing, is the hardware foundation of the system. The DHT11 moisture sensor, which monitors both humidity and temperature with dependable precision and minimal power consumption, is used to monitor environmental conditions.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.141281

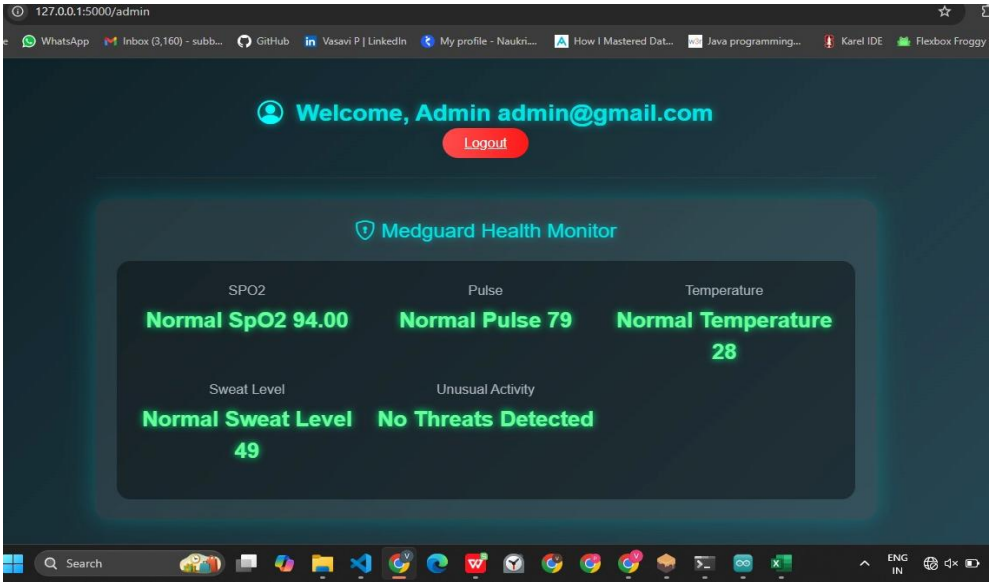

Figure 3: MedGuard Panel Showing Live Sensor Data

The ESP8266 NodeMCU development board, which offers embedded Wi-Fi connectivity, onboard CPU, and memory appropriate for Internet of Things applications, enables wireless data transmission. In order to minimize wiring complexity, real-time sensor data and system status are shown on a 16x2 LCD displays with an I2C interface. A pulse oximetry device sensor that measures hemoglobins that is oxygenated and deoxygenated using red and infrared LEDs is used to monitor oxygen saturation, providing precise SpO_2 measurements for health monitoring. These hardware and software elements work together to create a reliable and safe operational setting for the Med Guard Edge system.

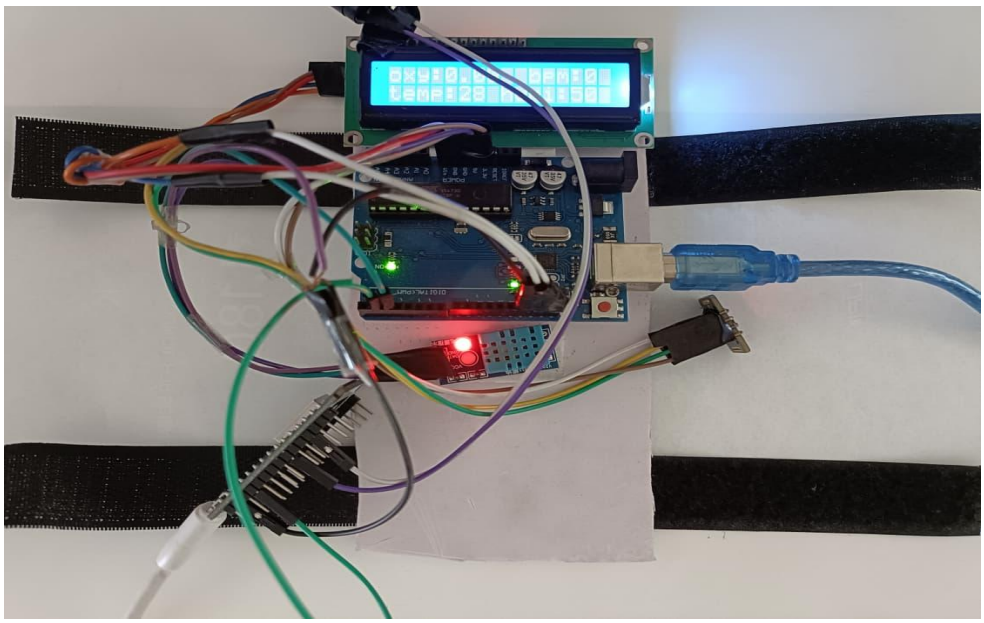

Figure 4: Hardware prototype showing Arduino uno with DHT 11, ESP8266 NodeMCU Board, LCD 16X2 Display, Oxygen sensor

VIII. MODULES

8.1 Smart Hand Band Sensing Module

This module records temperature, humidity, SpO_2 and BPM in real time using an Arduino equipped with DHT11 and MAX30102 sensors. It preprocesses raw signals, looks for anomalies, sounds an emergency bell, and shows vital signs on a 16x2 LCD. After processing, the data is prepared and transferred to the NodeMCU for additional examination.

DOI: 10.17148/IJARCCE.2025.141281

8.2 Wi-Fi Communication NodeMCU Module

The Arduino sends formatted sensor data to the NodeMCU after creating a secure Wi-Fi connection. The values are transformed into JSON and sent via HTTP POST to the MedGuard server. It enables dependable and low latency exchange of information between the edge system by sending out alerts in response to the server's response.

8.3 Clustered Federated Learning (CFL) Module

CFL trains local models without sharing raw data by classifying IoT devices according to data proximity or similarity. To create a combined cluster model that enhances the global model, cluster heads incorporate local updates. This increases accuracy and scalability, enhances privacy, and uses less bandwidth.

8.4 Security and Validation Module for Blockchain

For unchangeable, impenetrable verification, this module stores all model updates on a blockchain. Smart contracts ensure transparent donation tracking and update authenticity. By preventing poisoning threats and decentralizing trust, it safeguards the federated learning workflow.

8.5 Real-Time Anomaly Detection Module

Identify anomalies like faked data or device breach, this module continuously examines sensor values, network activity, and model updates. To ensure prompt reaction to hardware and cyber risks, it logs events, flags questionable activity, and sends out alerts using ML-based detection algorithms.

8.6 Self-Healing & Auto-Isolation Module

The system automatically separates hacked or malfunctioning nodes and initiates recovery operations such as resets or reconfigurations. These self-healing solutions guarantee continuous availability and prevent errors from propagating. This enables reliable, ongoing healthcare monitoring even in the case of faults or attacks.

8.7 Server & API Processing Module

After receiving JSON payloads, the backend server verifies sensor parameters and compares them to medical thresholds. It logs important events for auditing, detects anomalies, and creates alarms. It guarantees precise and effective processing of health data by sending rapid feedback to IoT devices.

8.8 Web Dashboard Visualization Module

For ongoing patient evaluation, a real-time health monitoring dashboard shows temperature, sweat level, pulse rate, SpO_2, and anomaly status.

IX. PERFORMANCE EVALUATION

The performance outcomes of the MedGuard Edge framework concentrating on two key aspects: blockchain validation time and end-to-end latency. These parameters help assess how efficiently the system handles data as it moves through different stages such as sensing, communication, model training, blockchain verification, and dashboard visualization.

9.1 Blockchain Validation Time

The time taken to validate model updates on the blockchain was measured across five global training rounds. As illustrated in Figure.5, the validation time varied between 700 ms and 780 ms, with the third iteration showing the maximum delay.

Key Observations:

- The first iteration records the lowest delay (~700 ms), which reflects minimal congestion in the network.
- Iterations 2 and 3 show a slight rise in validation time, reaching up to ~ 780 ms, likely because of increasing model size or network load.
- A drop to ~ 700 ms in iteration 4 suggests improved efficiency when fewer updates are processed.
- Iteration 5 settles around ~760 ms, showing steady performance.

Summary: The blockchain verification process adds a predictable and manageable amount of overhead, making it suitable for real-time data validation in healthcare IoT applications.

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.141281

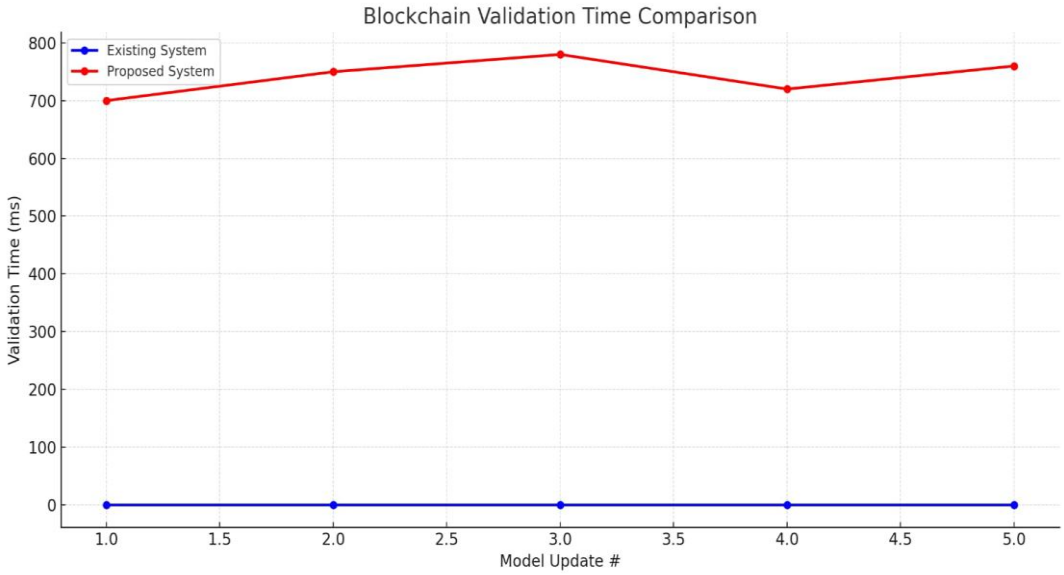

Figure 5: Blockchain Validation Time Across Consecutive Model Updates

End-to-End Latency Breakdown

To better understand how the total delay is distributed, each stage in the data flow was measured separately. Figure.6 shows the latency contribution from sensing devices to the dashboard output.

Latency Measurements:

- Sensor → NodeMCU: ~15 ms: Very low because the data transfer is direct and lightweight.
- NodeMCU → Server: ~60 ms: Delay occurs due to Wi-Fi transmission, JSON formatting, and communication overhead.
- Clustered Federated Learning: ~300 ms: Consists of both cluster-level aggregation and local model updates.
- Blockchain Validation: ~800 ms: The largest delay, caused by hashing operations, smart contract execution, and block confirmation.
- Dashboard Rendering: ~150 ms: Time taken for the server to send processed results and for the dashboard to update the visualization.

Summary: The total latency remains acceptable for continuous healthcare monitoring. With future optimizations—such as lighter consensus algorithms or faster blockchain networks—the overall delay can be further reduced.

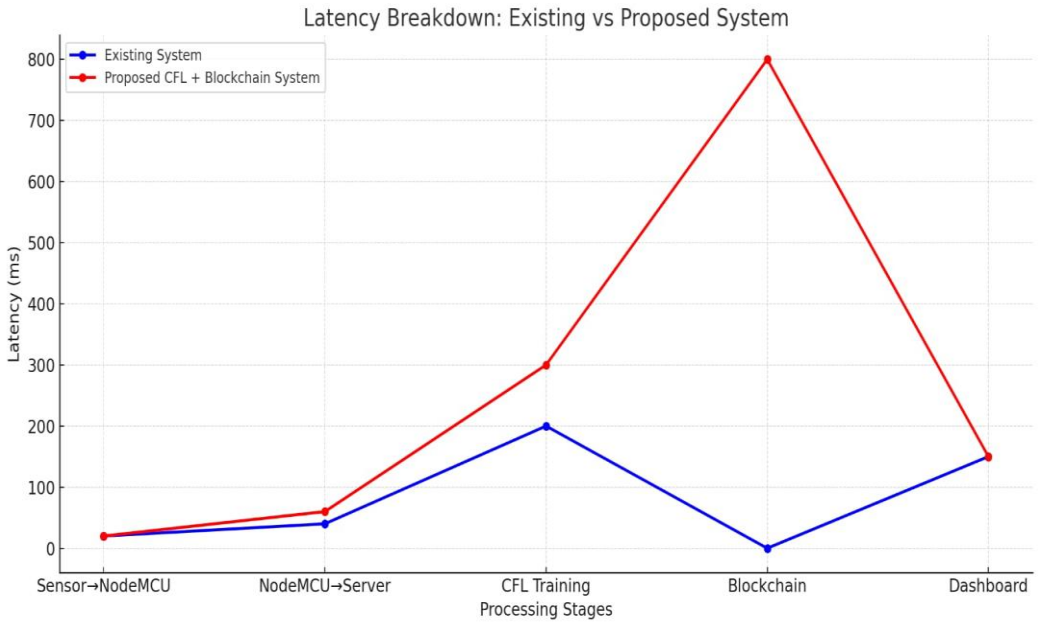

Figure 6: Latency Breakdown Across MedGuard Edge Pipeline

DOI: 10.17148/IJARCCE.2025.141281

X. CONCLUSION

A practical and forward-thinking approach to improving security and privacy in IoT technologies used in healthcare is provided by MedGuard Edge. Instead, then relying on centralized servers, it uses a decentralized architecture in which Clustered Federated Learning (CFL) and blockchain work together to keep confidential patient data on local devices. This combination ensures transparent, dependable, and tamper-resistant model updates while also protecting privacy. With the addition of IPFS-based storage, the system greatly improves data integrity and provides visible, verifiable records of every contribution made to the learning process.

By continuously monitoring physiological patterns and device behaviour, the system's real-time anomaly detection offers an extra degree of security by assisting in the early discovery of anomalous or possibly dangerous activities. Reliability is increased by its self-healing feature, which isolates compromised or failing nodes automatically and restores normal operation without human involvement. All things considered, MedGuard Edge is a significant advancement above conventional centralized healthcare IoT architectures. It improves security, increases privacy, scales effectively, and maintains dependability even under changing circumstances. The solution provides a strong basis for next-generation smart healthcare environments by integrating decentralized intelligence, continuous monitoring, and strong trust mechanisms. This ensures safe, real-time patient monitoring while protecting vital medical data from new cyber threats.

10.1 Future work

Future improvements to MedGuard Edge might focus on improving its intelligence, scalability, and practicality. Adaptive and context-sensitive clustering techniques that dynamically rearrange device groups according to data similarity, movement patterns, or clinical situations can be added to the clustered federated learning framework. The system's capacity to spot minute temporal variations in patient vitals and device behaviour may be further improved by including sophisticated deep learning-based anomaly detection models.

The blockchain architecture can be extended into a consortium or multi-institution network using optimized consensus algorithms and zero-knowledge proof procedures to increase throughput, lower latency, and offer more robust privacy guarantees in order to fortify the trust layer. In order to encourage sincere involvement and reliable federated learning updates across diverse healthcare nodes, future research may also investigate incentive-driven smart contracts.

To increase long-term dependability and usefulness, more research can concentrate on integrating redundant IPFS pinning techniques, fault-tolerant decentralized storage, and energy-efficient wearable hardware. System performance under practical operating settings may be further validated by extensive deployment throughout hospital networks and integration with 5G-enabled edge infrastructure. Lastly, adding more biological parameters to the sensing module and improving power management strategies may allow MedGuard Edge to be used in more clinical and emergency care situations.

ACKNOWLEDGMENT

The authors thank the faculty and staff of the Department of Information Science and Engineering at The Oxford College of Engineering for their advice and assistance. We are grateful to the open-source communities that support Web3, IPFS, and Ganache as well as to **Mrs. Visalini S.** for her technical advice and mentoring.

REFERENCES

[1]. R. Alami, L. M. Benhiba, K. El Yassini, and A. Oukaira, “Blockchain-Enabled Federated Learning for Detection of Malicious IoT Nodes,” *IEEE Access*, 2024.
[2]. M. H. Alsamhi et al., “Federated Learning Meets Blockchain in Decentralized Data-Sharing: Healthcare Use Case,” *IEEE Internet of Things Journal*, 2024.
[3]. F. Zhou, K. Li, and Y. Xu, “BIT-FL: Blockchain-Enabled Incentivized Federated Learning Framework,” *IEEE Transactions on Mobile Computing*, 2024.
[4]. S. Yuan, H. Chen, and D. Wu, “Secure and Efficient Federated Learning through Layering and Sharding Blockchain,” *IEEE Transactions on Network Science and Engineering*, 2024.
[5]. R. Lin, P. Xia, and Y. Wang, “Time-Efficient Blockchain-Based Federated Learning,” *IEEE/ACM Transactions on Networking*, 2024.
[6]. Y. Huang, X. Lin, and Z. Wang, “FLchain: Federated Learning and Blockchain Empowered Security Architecture for IoT Healthcare,” *IEEE Internet of Things Journal*, 2023.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025
DOI: 10.17148/IJARCCE.2025.141281

[7]. S. T. Ahmed, K. B. Al-Dahlaki, and M. H. Ali, "Towards Blockchain-Based Federated Learning in Categorizing Healthcare Monitoring Devices," *BMC Medical Imaging*, 2024.
[8]. N. Dong, Q. Li, and T. Zhang, "Defending Against Poisoning Attacks in Federated Learning with Blockchain," *IEEE Transactions on Artificial Intelligence*, 2024.
[9]. X. Yang and Z. Xing, "Federated Medical Learning Framework Based on Blockchain and Homomorphic Encryption," *Wiley Journal of Healthcare Informatics*, 2023.
[10]. L. T. Fang, M. Ling, and C. Y. Koo, "Enhancing IoT with Federated Learning and Blockchain-Based Authentication," *International Journal of Electrical, Electronics and Computer Science (IJEEMCS)*, 2025.
[11]. A. Sharma and R. Gupta, "Cybersecurity Challenges in Healthcare IoT Systems: An Overview," *IEEE Communications Surveys & Tutorials*, 2023.
[12]. J. He, S. Zhao, and P. Xu, "Anomaly Detection Techniques for IoT-Based Health Monitoring Systems," *IEEE Sensors Journal*, 2024.
[13]. M. Chen and Y. Hao, "Edge Computing for Smart Healthcare: Federated Learning Approaches," *IEEE Network*, 2023.
[14]. V. Reddy and P. Kumar, "A Survey on Blockchain Security Models for IoT Networks," *IEEE Access*, 2022. MedGuard Edge: Intelligent Cyber Defense for Healthcare IoT Devices
[15]. S. Li, H. Zhu, and Y. Jin, "Securing Distributed IoT Systems Using Blockchain and Machine Learning," *IEEE Transactions on Industrial Informatics*, 2023.
[16]. K. Xu and L. Zhao, "Self-Healing IoT Networks Using Machine Learning," *International Journal of Distributed Sensor Networks*, 2023.
[17]. P. Singh and A. Jain, "Federated Learning for Health Data Privacy Preservation," *Health Informatics Journal*, 2023.
[18]. S. Bhalekar and T. Shah, "Blockchain for Healthcare Data Security: A Review," *Journal of Medical Systems*, 2024.
[19]. M. V. Raghu and S. Rekha, "Wearable Medical IoT Devices for Vital Monitoring," *Biomedical Engineering Letters*, 2023.
[20]. T. Kale and P. Salian, "IoT-Based Remote Health Monitoring: Design and Implementation," *International Journal of Smart Sensor Technologies*, 2022.

 This work is licensed under a Creative Commons Attribution 4.0 International License