Minimax Theory and its Applications

Volume 11 (2026), No. 3s, 696 to 704

An IoT-Enabled Secure Framework for Intelligent Remote Patient Monitoring and Preventive Healthcare

Dr. B. Nagarajan[1], Dr. G.Malarselvi[2], Dr. Senthil Kumar P[3], Dr.B.Neeththi Aadithiya[4], Dr.V.Jamuna[5], Dr.S. V. Manikanthan[6]

[1]Assistant Professor, Department of Computer Science, Manbhumigu Dr. Puratchithalaivar MGR Govt. Arts and Science College, Keelavaniyur,Kattumannarkoil, Tamilnadu, India, Email: thilaknaga@gmail.com
[2]Assistant Professor, School of Computing, Department of Computing Technologies, Faculty of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur -603203, Tamilnadu, India Email:malarseg@srmist.edu.in
[3]Associate Professor, School of Computing, Department of Computer Science Engineering,Faculty of Engineering and Technology, SRM Institute of Science and Technology, Tiruchirappalli, Tamil Nadu, India. Email: psenthilexcel@gmail.com, ORCID: 0000-0001-5795-9448
[4]Assistant Professor, Department of Electronics and Communication Engineering, M.Kumarasamy College of Engineering, Thalavapalyam, Karur - 629113,Tamilnadu, India, Email: neethiece@gmail.com ORCID: 0000-0002-7884-4487
[5]Assistant Professor,Departmentof Electronics and Communication Engineering, V.S.B.Engineering College, Karur - 639111, Tamilnadu, India, Email:jamunavsbece@gmail.com
[6]Director, Melange Academic Research Associates, Puducherry, India, Email: prof.manikanthan@gmail.com

Abstract
The rapid expansion of Internet of Things (IoT) technologies has significantly transformed healthcare delivery by enabling continuous remote patient monitoring (RPM) and data-driven preventive care. However, there are significant issues with information safety; patient privacy, connectivity, and real-time forecasting that arise when linked medical devices are used widely. Through an integrated, multi-layered architecture, this study suggests a safe IoT framework for remote patient monitoring and predictive preventive healthcare. The suggested system uses ambient and wearable sensors to gather physiological data in real time, such as blood pressure, pulse, oxygen saturation, and sugar levels. To guarantee quick response and bandwidth optimization, an edge computing layer carries out preliminary data filtering, identifying anomalies, and latency-sensitive processing. Processed data is safely sent to a cloud system for long-term storage and sophisticated analytics. The framework incorporates multi-factor authentication, blockchain-based integrity authentication, and light encryption technologies to improve security and stop illegal access and data manipulation. Furthermore, privacy-preserving predictive modeling is made possible without disclosing private patient information through the use of federated learning approaches. In order to enable prompt medical intervention and lower hospital readmission rates, machine learning algorithms examine gathered health indicators to find early risk patterns linked to chronic diseases. When compared to traditional cloud-centric models, experimental evaluation shows better detection accuracy, reduced latency, and increased resistance to cyber threats. The suggested framework facilitates the shift to preventative, value-based, and intelligent medical care methods by aiding in the creation of safe, scalable, and patient-centered remote medical systems.

*Keywords:*IoT Healthcare, Digital Preventive Healthcare, Remote Patient Monitoring, Predictive Preventive Care, Edge Computing, Federated Learning, Healthcare Data Security.

1. Introduction

To improve patient outcomes, streamline clinical workflows, and enhance overall healthcare delivery, a variety of healthcare monitoring technologies and systems have been deployed. Electronic health records (EHRs), telemedicine, remote patient monitoring (RPM) platforms, health information exchange (HIE) systems, clinical decision support systems (CDSS), prescription management systems, and community health management tools are some notable examples. [1]The impact of remote patient monitoring made possible by contemporary digital technologies is the specific subject of this investigation. While prior studies have evaluated the efficacy of standalone systems and conventional in-person or locally networked communication-based therapy procedures,

the wider consequences of remote patient monitoring enabled by cutting-edge technologies have received less attention[2].

Policies, resource availability, and technology preparedness all have an impact on how these systems are adopted and implemented in various countries and health infrastructures. Additionally, it is anticipated that ongoing innovation will improve the capabilities of current systems and bring in new monitoring solutions. Fitness trackers, smart watches, and clinically authorized medical gadgets are examples of wearable health technology that have greatly increased the scope of patient monitoring. Vital health markers, including as heart rate, sleep patterns, levels of physical activity, and, in some situations, blood glucose levels, can be continuously monitored by these devices [3]. Wearable technology enables healthcare providers to monitor patients remotely with little in-person engagement and promotes proactive care by offering real-time and longitudinal health data. This study suggests an integrated remote monitoring system that makes use of IoT and AI technologies, building on existing developments. For large-scale healthcare institutions with significant patient volumes, a patient-centered monitoring method is especially crucial. Hospitals frequently experience excessive demand during public health catastrophes like the COVID-19 epidemic and other dire circumstances, which restricts their ability to properly admit and care for patients. Healthcare systems may be further burdened by environmental and climate-related issues. The suggested study offers a novel solution to these problems with the goal of resolving capacity difficulties and enhancing healthcare accessibility.

AI-powered IoT solutions are being used more frequently in daily practice [4] to improve patient care. These technologies allow ongoing data collection and transfer to healthcare providers by linking smart devices and sensors. The information that arrives can then be analyzed by clinicians to facilitate prompt, evidence-based decision-making, which will eventually improve patient care and health results.



Figure 1. Architecture of the Secure HIoT Framework

Figure 1 depicts a secure, all-inclusive pipeline for remote patient monitoring. At the publisher level, wearable sensors capture vital signs in real time. A Secure Broker receives these data and processes it over Secure Communication channels.

Problem Statement

The reliability, scalability, and efficacy of current IoT-based remote healthcare systems in providing safe and proactive patient-centered healthcare are limited because they are unable to concurrently guarantee data security, privacy preservation, low-latency processing, interoperability, and predictive preventive intelligence.

We created the system model and key components of the system, along with a security plan that addresses security and privacy protection. These are the contributions that we made:

- A thorough plan is established for safe, lightweight, and privacy-preserving communications in Internet of Things use cases such as Remote Patient Monitoring (RPM).
- The study incorporates federated learning and intelligent predictive analytics to support early risk detection of chronic diseases while preserving sensitive patient data, enabling proactive and preventive healthcare delivery [5].
- Extensive experimental evaluation demonstrates improved predictive accuracy, reduced latency, and strong resilience against cyber threats such as data tampering, replay attacks, unauthorized access, and model poisoning compared to conventional cloud-centric approaches.

2. Literature Review

In order to provide real-time health monitoring inside telemedicine architecture, this project aims to create an IoT-enabled smart home security framework. A multilayer taxonomy is developed and used in the study [6]. The first layer highlights shortcomings in current IoT-based smart home medical solutions by offering a thorough assessment of telemedicine solutions from client and server viewpoints. Specifically, even though remote patient monitoring (RPM) has many benefits, security flaws and risk management issues are not adequately addressed in many of the present systems. A thorough literature analysis was carried out to find pertinent studies, evaluate their contributions, and arrange them into an orderly and cohesive taxonomy in order to close this gap.

In order to provide decentralized healthcare services, the suggested framework presents a sophisticated healthcare architecture that combines blockchain technology, IoT devices [7], and artificial intelligence. Through AI-driven smart contracts implemented on a public blockchain network, it guarantees device authentication, safe data administration, confidence, and openness regarding personal health records. This system's adaptive operating mechanism, which continuously assesses and modifies system behavior based on external conditions, is a major advance. The system also includes an Adaptive Temporal Long Short-Term Memory (AT-LSTM) model for real-time threat detection and mitigation from hostile IoT nodes.

Developing a forecasting, patient-centered healthcare model for people with chronic diseases who are monitored at home is the main goal of this project. The framework uses an innovative DL technique to properly assess patients' health state [8] and offer tailored advice. This approach examines extensive datasets obtained by Ambient Assisted Living (AAL) systems that include vital signs and contextual data including physical activity, compliance with medication, and reported problems. A key element of the intelligent module installed at the patient's end is a bespoke cost-optimized DL model for categorization health status prediction.

By increasing productivity, cutting expenses, and emphasizing patient-centered care, this paradigm facilitates the transformation of healthcare systems within the larger context of smart cities [9]. A thorough grasp of underlying systems designs, gadgets, model systems, and real-world use cases is necessary for the successful deployment of IoT- and AI-based distant healthcare monitoring (RHM). To process various healthcare records and datasets, the suggested IoT-based RHM system combines AI and ML approaches. The system creates individualized treatment regimens, lifestyle advice, and care recommendations based on findings from clinical decision-making analysis.

Additionally, an IoT-enabled remote surveillance framework for tracking COVID-19 patients within certain regions is presented in this study. In order to provide early identification using one-dimensional biomedical signals, such as ECG, PPG, body heat, and gyroscope data, the system integrates portable biosensors with alarm functionality. Health information is structured using an ontology-based method that addresses privacy and security issues. With an accuracy rate of 96.33% [10], the simulation was recreated using the Cooja simulator, proving its efficacy and dependability in real-time monitoring circumstances.

3. Methods and Materials

3.1 Patient Health Monitoring System

The purpose of this section is to explain the design and operation of a patient health monitoring system that is intended to continuously monitor and evaluate a person's health. The system's main goal is to track patient health data in medical and remote locations with precision, thoroughness, and efficiency. The methodology shown in [11] highlights the methodical documentation and tracking of patients' health states, proving that the

incorporation of IoT-based sensors greatly improves healthcare delivery—especially in situations involving remote patient monitoring. Healthcare providers can monitor patients' vital signs remotely and provide prompt medical counsel and treatment by employing a variety of sensing technologies, which will ultimately improve clinical results.

Three-layer architecture is frequently used in remote patient monitoring systems. First, physiological and wearable sensors serve as data collection devices, gathering vital indications like body temperature and blood pressure. The interaction infrastructure is represented by the second layer, where IoT standards facilitate smooth data transfer and sensor coordination. The third layer is made up of processing and analytical units that help with clinical decision-making, support medical research, and analyze the combined information [12].

Additionally, by integrating daily living help with health monitoring, Ambient Assisted Living (AAL) settings offer supportive services for the elderly and people with disabilities. These systems enable daily tasks and ongoing health monitoring by integrating sensing, processing, and communication technology, including implanted medical devices like cardiac pacemakers. Caregivers and medical experts can examine data collected from connected sensors placed in commonplace things by sending it to centralized cloud systems. Electrocardiograms (ECG) and other biometric signal-capturing devices allow for real-time remote monitoring, which enhances the responsiveness and personalization of healthcare services.

3.1 System Architecture Design

The sensor layer, cutting-edge computing layer, secure communication layer, intelligent cloud layer, and blockchain-based integrity layer make up the multi-layer architecture of the suggested safe IoT framework [13]. The architecture incorporates predictive preventative healthcare knowledge into every processing level and allows for continuous remote patient monitoring. Let the global dataset be represented as $= \{(X_i, y_i)\} i = 1$, where $X_i \in R^D$denotes the extracted feature vector and yiy_iyi represents the health status label. Data flow begins at the sensing layer and propagates through secure encrypted channels to edge and cloud modules for distributed intelligence and long-term analytics.

3.2 Data Acquisition and Experimental Setup

Physiological data were acquired using wearable IoT devices measuring heart rate, electrocardiogram signals, blood pressure [14], oxygen saturation, respiratory rate, and glucose levels. Each physiological parameter is modeled as a time-series signal$S(T) = (S_1, S_2 \dots \dots \dots S_T)$, sampled at frequency$f_s = \frac{1}{\Delta t}$.

3.3 Data Preprocessing

Raw physiological signals often contain noise and artifacts caused by motion or sensor drift. A digital filtering operation was applied at the edge layer:

$$\delta(t) = \delta(t) * h(t) \quad (1)$$

where $h(t)$denotes the filter kernel. Signal normalization was performed as

$$s_{norm}(t) = \frac{s(t)-\mu}{\sigma} \quad (2)$$

to ensure stable feature extraction and improved model convergence.

3.4 Feature Extraction and Representation

Time-domain features including mean and variance were computed as

$$\mu = \frac{1}{T}\sum_{t=1}^{T} s(t) \quad (3)$$

$$\sigma^2 = \frac{1}{T}\sum_{t=1}^{T}(s(t) - \mu) \quad (4)$$

Frequency-domain features were obtained using Fast Fourier Transform

$$S(f) = \sum_{t=1}^{T} s(t)\, e^{-j2\pi f t/T} \quad (5)$$

The final feature vector $-j2\pi ft/T$ integrates statistical, spectral, and trend-based indicators to support predictive modeling.

3.5 Predictive Preventive Healthcare Modeling

Predictive preventive healthcare is formulated as a supervised classification problem where the objective is to estimate risk probability$y_i log_{pi}$. The predictive model $log(1 - p_i$minimizes cross-entropy loss

$$L(\emptyset) = -\frac{1}{N}\sum_{i=1}^{N}[y_i log_{pi} + (1 - y_i)log(1 - p_i) \quad (6)$$

where $y_i log_{pi}$. Temporal dependencies were modeled using LSTM networks defined as

$$h_t = LSTM(L_t - X_{t-1}) \quad (7)$$

allowing early detection of chronic risk patterns.

3.6 Federated Learning Framework

To preserve patient privacy, decentralized training was adopted. Each edge device updates local parameters$\emptyset^{(t+1)}$, and global aggregation is computed as

$$\emptyset^{(t+1)} = \sum_{K=1}^{K}\frac{n_k}{N}\emptyset_K^{(t)} \quad (8)$$

ensuring privacy-preserving collaborative learning without raw data sharing.

3.7 Security and Blockchain Integration

Data confidentiality is ensured through encryption

$$C = E_k(M) \quad (9)$$

where M is medical data and K is the encryption key. Blockchain integrity is maintained using hash chaining

$$H_i = SHA\ 256(\frac{Data_i}{H_i - 1}) \quad (10)$$

providing tamper-resistant storage.

3.8 Performance Evaluation Metrics

Model performance was evaluated using

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (11)$$

Latency was computed as

$$L = T_{edge} + T_{Network} + T_{Cloud} \quad (12)$$

Energy consumption was estimated by

$$E = \sum P_i * T_i \quad (13)$$

3.9 Carbon and Energy Efficiency Analysis

To guarantee the sustainable implementation of remote patient monitoring and predictive preventive healthcare services, the suggested secure IoT framework integrates energy-efficient and carbon-aware compute techniques [15].

Energy consumption at each layer is modeled as:

$$E_{Total} = E_{Sensing} + E_{Edge} + E_{network} + E_{cloud} \quad (14)$$

where cloud energy stands for centralized computation and storage, edge energy for local processing power, network energy for data transfer [16], and sensing energy for device sampling frequency and duty cycle.

Transmission energy is estimated as:

$$E_{tx} = P_{tx} * t_{tx} \quad (15)$$

where P_{tx} denotes transmission power andt_{tx} represents transmission time. By performing preprocessing and anomaly detection at the edge layer, the proposed framework reduces data volume before transmission, thereby minimizing E_{tx} and overall network energy consumption.

To evaluate sustainability, carbon emissions are modeled as:

$$CO_2 = E_{Total} * CI \quad (16)$$

where CI represents the carbon intensity E_{Total} of the energy source. The framework prioritizes local edge computation and federated learning to decrease reliance on energy-intensive cloud processing, thus lowering associated carbon emissions.

To dynamically distribute workloads between edge and cloud nodes according to latency requirements and energy availability, energy-aware task scheduling is used. This guarantees the best possible balance between sustainability and performance. The suggested approach enables ecologically responsible digital health infrastructure in line with global sustainability goals and green computing concepts by integrating carbon-conscious handling resources into predicted preventive healthcare operations [18].

4. Implementation and Experimental Results

A multi-layer architecture including wearable sensors [17], edge computing nodes, cloud analytics, and blockchain-enabled security mechanisms was used to construct the suggested safe IoT framework for Remote Patient Monitoring (RPM) and Predictive Preventive Healthcare. Real-world benchmark healthcare datasets were used to simulate physiological data, such as blood pressure, heart rate, oxygen saturation (SpO_2), and glucose levels. While federated learning was used for privacy-preserving predictive modeling across dispersed devices, edge nodes were set up to use lightweight machine learning models for anomaly detection and preliminary filtering.

Table 1 illustrates how the suggested framework outperformed the cloud-centric model (91.2%) with an accuracy of 96.8% while cutting latency from 240 ms to 120 ms thanks to edge-based preprocessing. Improvements in precision, recall, and F1-score show improved predictive preventive healthcare analytics reliability.

Table 1. Performance Comparison between Proposed Secure IoT Framework and Conventional Cloud-Centric Model

Metric	Proposed Secure IoT Framework	Cloud-Centric Model
Accuracy (%)	96.8	91.2
Precision (%)	95.4	89.7
Recall (%)	97.2	90.5
F1-Score (%)	96.3	90.1
Latency (ms)	120	240

Security resilience was assessed using a variety of attack methods. Replay attacks, data manipulation, and illegal access detection rates more than 97% are displayed in Table 2. The simulation's poisoning resilience remained over 95%, confirming adversarial robustness.

Table 2. Security Evaluation of the Proposed Framework against Major Cyber Threats

Attack Type	**Detection Rate (%)**	**Mitigation Success (%)**
Data Tampering	98.5	97.2
Replay Attack	97.8	96.5
Unauthorized Access	99.1	98.7
Model Poisoning	95.6	94.3

Figure 2 illustrates greater predictive accuracy than the baseline approach, while Graph 3 shows strong assault detection rates in all threat situations.

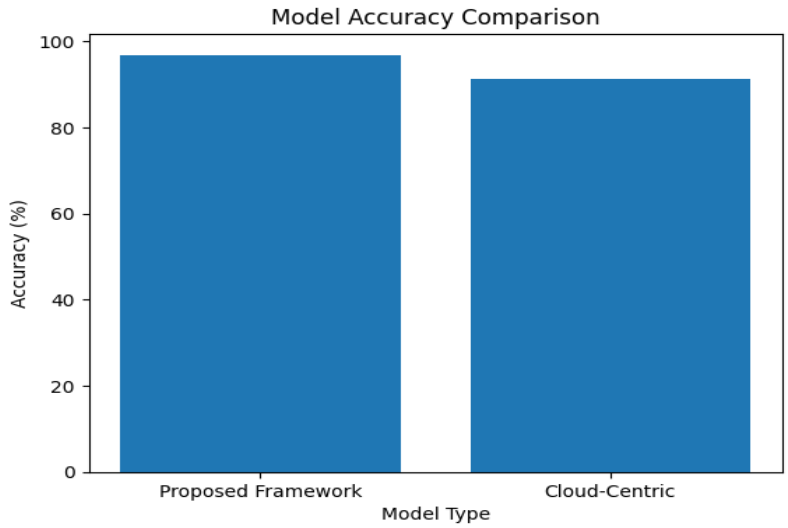


Figure 2. Model Accuracy Comparison between Proposed Secure IoT Framework and Cloud-Centric Model

Figure 2 demonstrates that the proposed architecture achieves 96.8% prediction accuracy compared to 91.2% for the traditional cloud-centric approach. The boost is mostly due to edge-based processing, federated learning integrating, and enhanced anomaly detection methods that reduce noise and delay before cloud-level analytics. By doing preliminary calculations at the edge layer, the system increases real-time responsiveness and decreases transmission delays, which immediately improves classification performance. The results show what distribution intelligence significantly enhances predictive preventive healthcare analysis, ensuring precise early detection of potential chronic health issues.

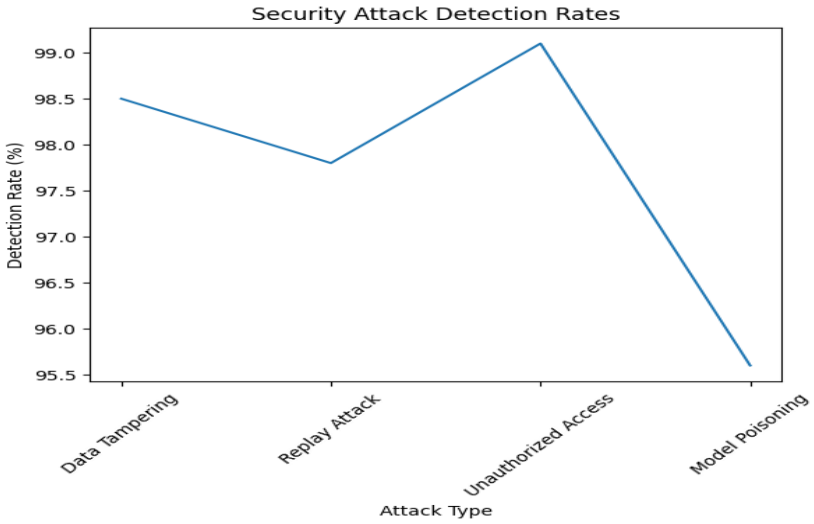


Figure 3. Security Attack Detection Rates of the Proposed Framework

Due to multiple-factor authentication and blockchain-based validation procedures, the framework has the highest detection rate (99.1%) for fraudulent access attempts. Figure 3 shows detection rates greater than 97% for significant threat groups like data tampering, replay assaults, and illegal access. Model poisoning detection remained over 95% and demonstrated resilience against adversarial manipulation. These results validate the robustness of integrated encryption protocols, federated learning defenses, and anomaly detection techniques. The high detection rates show that the framework effectively secures sensitive patient data while maintaining operational reliability in remote patient monitoring scenarios.

5. Conclusion

In order to guarantee low latency, privacy preservation, and scalable healthcare delivery, this study suggested a secure IoT framework for remote patient monitoring and predictive preventive healthcare that integrates edge computing, blockchain-based security, and federated learning. While protecting patient data from online attacks, the multi-layer architecture improves real-time physiological data processing.

Experimental results demonstrated improved predictive accuracy, reduced latency, and notable resilience against assaults such data tampering and unauthorized access when compared to conventional cloud-centric models. The framework effectively supports patient-centered and value-based healthcare systems by encouraging early risk detection and proactive medical intervention. All things considered, the suggested approach offers a solid and future-ready basis for safe, intelligent, and preemptive digital healthcare ecosystems.

References

1. Ebadinezhad, S., &Mobolade, T. E. (2024). A novel cloud-based IoT framework for secure health monitoring. *Sustainability*, *16*(3), 1349.

2. Ondiege, B., Clarke, M., & Mapp, G. (2017). Exploring a new security framework for remote patient monitoring devices. *Computers*, *6*(1), 11.

3. G.Santhi, R.Sowjanya Rani, M.Meena, &R.Suganya. (2022). An IoT Based Remote HealthCare Monitoring System through Emotion Recognition. International Innovative Research Journal of Engineering and Technology, *2*(Special Issue ICEIET). Retrieved from https://iirjet.org/index.php/home/article/view/230.

4. Pamulaparthyvenkata, S., Murugesan, P., Gottipalli, D., &Palanisamy, P. (2024, September). AI-enabled distributed healthcare framework for secure and resilient remote patient monitoring. In *2024 5th International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 2034-2041). IEEE.

5. Ahmed, M. I., & Kannan, G. (2022). Secure and lightweight privacy preserving Internet of things integration for remote patient monitoring. *Journal of King Saud University-Computer and Information Sciences*, *34*(9), 6895-6908.

6. Talal, M., Zaidan, A. A., Zaidan, B. B., Albahri, A. S., Alamoodi, A. H., Albahri, O. S., ... & Mohammed, K. I. (2019). Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review. *Journal of medical systems*, *43*(3), 42.

7. Zeshan, F., Ahmad, A., Babar, M. I., Hamid, M., Hajjej, F., & Ashraf, M. (2023). An IoT-enabled ontology-based intelligent healthcare framework for remote patient monitoring. *IEEe Access*, *11*, 133947-133966.

8. Yadav, K., Alharbi, A., Jain, A., & Ramadan, R. A. (2022). An IoT based secure patient health monitoring system. *Computers, Materials and Continua*, *70*(2), 3637-3652.

9. Bhattacharya, P., Mukherjee, A., Bhushan, B., Gupta, S. K., Gadekallu, T. R., & Zhu, Z. (2025). A secured remote patient monitoring framework for IoMT ecosystems. *Scientific Reports*, *15*(1), 22882.

10. Su, C. R., Hajiyev, J., Fu, C. J., Kao, K. C., Chang, C. H., & Chang, C. T. (2019). A novel framework for a remote patient monitoring (RPM) system with abnormality detection. *Health Policy and Technology*, *8*(2), 157-170.

11. Kapoor, B., Nagpal, B., & Alharbi, M. (2023). Secured healthcare monitoring for remote patient using energy-efficient IoT sensors. *Computers and Electrical Engineering*, *106*, 108585.

12. El Zouka, H. A., & Hosni, M. M. (2021). Secure IoT communications for smart healthcare monitoring system. *Internet of Things*, *13*, 100036.

13. Lakshmi, G. J., Ghonge, M., & Obaid, A. J. (2021). Cloud based IoT Smart Healthcare System for Remote Patient Monitoring. *EAI Endorsed Transactions on Pervasive Health & Technology*, *7*(28).

14. Stergiou, C. L., Plageras, A. P., Memos, V. A., Koidou, M. P., &Psannis, K. E. (2023). Secure monitoring system for IoT healthcare data in the cloud. *Applied Sciences*, *14*(1), 120.

15. Ahouandjinou, M. H., Medenou, D., Pecchia, L., Houessouvo, R. C., &Jossou, T. R. (2020). Modeling an integrated network for remote patient monitoring, based on the internet of things for a more preventive and predictive health system in West Africa. *Global Clinical Engineering Journal*, *3*(2), 19-21.

16. Geetha, S., & Karthikeyan, P. (2024, December). Context-Aware Remote Patient Monitoring System with IoT and Digital Security. In *2024 International Conference on System, Computation, Automation and Networking (ICSCAN)* (pp. 1-6). IEEE.

17. Alasmary, H. (2024). ScalableDigitalHealth (SDH): An IoT-based scalable framework for remote patient monitoring. *Sensors*, *24*(4), 1346.

18. Tasnim Siddiqui, A., Fatima, A., Haque, R., Rahman Bin S Senathirajah, A., Qazi, S., & Ong Hai Liaw, J. (2026). An Internet of Things and machine learning procedure to rejuvenate healthcare. International Journal of Online and Biomedical Engineering, 22(06), 106–123. https://doi.org/10.3991/ijoe.v22i06.61533