International Journal of Artificial Intelligence and Computer Electronics
Volume: 02, Issue: 03, July-September 2026, pp:114-124
P-ISSN 3117-8529 | E-ISSN 3117-8537

Secure And Decentralized Health Data Management Using IoMT And Blockchain

Mohammed Wasif Ur Rahman[2], Mr. Mohammed Rahmat Ali[2]
[1]PG Scholar, Department Of Computer Science & Engineering, ISL Engineering College, Hyderabad, India. India.
[2] Assistant Professor, Department Of Computer Science & Engineering, ISL Engineering College, Hyderabad, India.

Corresponding Author Email: mohammedwasif008@gmail.com

Article Received 24-06-2026, Revised 21-07-2026, Accepted 17-08-2026

ABSTRACT
The rapid growth of the Internet of Medical Things (IoMT) is transforming modern healthcare by enabling continuous patient monitoring, early disease detection, and improved clinical decision-making. However, healthcare data is often distributed across multiple hospitals, medical institutions, and digital platforms, creating significant challenges related to interoperability, secure data sharing, privacy, and efficient data management. To address these issues, this project proposes a blockchain-enabled framework for the secure, interoperable, and privacy-preserving validation and storage of IoMT-generated healthcare data. The proposed system utilizes Hyperledger Fabric, a permissioned blockchain platform, to provide controlled access, tamper-resistant data management, secure transactions, and transparent auditing within healthcare environments. Edge computing is also incorporated to process data closer to IoMT devices, thereby reducing communication latency, minimizing network congestion, and improving the efficiency of real-time healthcare services. The decentralized architecture enables authorized healthcare stakeholders to securely exchange patient information while maintaining data integrity, confidentiality, and privacy. The framework can support important applications such as remote patient monitoring, preventive healthcare, and timely clinical intervention. Experimental evaluation indicates that the proposed approach has the potential to enhance healthcare workflow efficiency, accelerate clinical decision-making, and support a more patient-centered model of healthcare data management. Overall, the proposed framework contributes toward the development of a secure, scalable, interoperable, and efficient digital healthcare infrastructure for future IoMT-based healthcare systems.

Keywords: *Internet of Medical Things (IoMT), Blockchain, Hyperledger Fabric, Edge Computing, Healthcare Data Security, Interoperability, Privacy Preservation, Remote Patient Monitoring, Secure Data Storage, Digital Healthcare.*

1. Introduction

The rapid development of the Internet of Medical Things (IoMT) has changed the way healthcare information is generated, collected, transmitted, and utilized. IoMT connects medical sensors, wearable devices, monitoring equipment, healthcare applications, and clinical information systems to support continuous observation of patients and timely access to medical information. These technologies can improve remote monitoring and assist healthcare professionals in making informed decisions. At the same time, the increasing volume of medical information generated by connected devices creates significant challenges concerning data confidentiality, integrity, privacy, interoperability, and secure information exchange. Islam et al. highlighted the broad potential of connected healthcare systems while also identifying security, privacy, interoperability, and management as important concerns in IoT-enabled healthcare environments [1].

Healthcare data differs from many other categories of digital information because it contains highly sensitive personal and clinical information. Patient records, diagnostic reports, physiological measurements, prescriptions, and monitoring data must be protected against unauthorized access and manipulation. A security breach can affect not only the confidentiality of an individual but also the reliability of clinical decisions based on compromised information. Saba et al. investigated secure and energy-efficient IoMT-based healthcare environments and emphasized the importance of protecting medical information while considering the limited resources of connected healthcare devices [2]. Therefore, future healthcare infrastructures require security mechanisms that can operate efficiently while maintaining strong protection for sensitive patient information.

The heterogeneous nature of IoMT environments further complicates healthcare data management. Medical devices may use different communication protocols, data formats, and computational platforms, while healthcare information can be distributed among hospitals, laboratories, clinics, cloud platforms, and individual healthcare providers. This fragmentation can make secure data sharing difficult and may result in isolated information repositories. Baker et al. discussed the technologies, challenges, and opportunities associated with IoT-enabled smart healthcare and highlighted interoperability, security, scalability, and reliable communication as important requirements for connected healthcare systems [3].

Cloud-based healthcare platforms have provided considerable storage and processing capabilities for medical applications, but centralized architectures can introduce additional security and availability concerns. When large volumes of patient information are maintained by a centralized service, the failure or compromise of that service can affect access to critical information. Moreover, centralized control can create difficulties in establishing transparent records of data access and modification. Distributed technologies therefore offer an alternative approach in which information transactions can be recorded across a trusted network of participating entities.

Blockchain technology has attracted considerable attention as a potential solution for secure healthcare data management. Its distributed ledger structure can provide tamper-resistant transaction records and support transparent verification of data-related operations. Instead of relying exclusively on a central authority, blockchain allows authorized participants to maintain a synchronized record of transactions. This characteristic can be valuable in healthcare environments where multiple organizations need to exchange information while maintaining accountability and data integrity.

Permissioned blockchain platforms are particularly relevant to healthcare because medical information cannot normally be exposed to unrestricted public participation. **Hyperledger Fabric** provides a permissioned blockchain architecture in which participating organizations can be identified and access policies can be established. Such controlled participation can support secure healthcare collaboration while providing an auditable record of transactions. Jamil et al. demonstrated the potential of combining IoT, blockchain, and healthcare monitoring to protect the integrity of patient vital-sign information in smart hospital environments [4].

The integration of blockchain with edge computing provides another opportunity to improve IoMT data management. IoMT devices continuously generate physiological measurements, and transferring all raw information to a remote cloud infrastructure can increase communication latency and network traffic. Edge computing allows selected processing operations to be performed closer to the data source. This can reduce the amount of information transmitted to remote servers and enable time-sensitive healthcare applications to respond more rapidly. Sekaran et al. investigated blockchain-based mobile edge computing for IoT automation and demonstrated the relevance of combining distributed ledger technologies with edge-based processing [5].

Privacy protection remains an essential requirement when blockchain is applied to healthcare. Although blockchain can provide strong integrity and traceability, storing sensitive patient information directly on a distributed ledger may create privacy concerns because blockchain records are intended to be persistent. Consequently, an appropriate healthcare architecture should distinguish between sensitive clinical information and the metadata required for verification and auditing. Habib et al. examined privacy protection for medical data in heterogeneous IoMT environments and highlighted the need for security mechanisms capable of addressing internal as well as external threats [6].

The integration of IoT and blockchain can also improve trust between healthcare organizations. Satamraju investigated the integration of IoT and blockchain in healthcare and demonstrated the feasibility of using blockchain as part of a scalable healthcare architecture [7]. Such integration can support controlled data exchange, transaction verification, and traceability while reducing dependence on a single centralized repository.

The emergence of advanced healthcare applications has further increased the need for trustworthy and interoperable digital infrastructures. Emerging technologies such as edge computing, blockchain, artificial intelligence, and advanced communication networks can operate together to support remote monitoring, intelligent diagnosis, and personalized healthcare. Manogaran et al. discussed emerging trends and challenges associated with IoMT and wireless healthcare networks, emphasizing the complexity of building secure and efficient connected healthcare infrastructures [8].

Despite these developments, existing approaches often address individual challenges rather than providing a unified framework for secure, decentralized, and efficient healthcare data management. A healthcare system requires not only data protection but also controlled access, interoperability, low-latency processing, transaction traceability, and reliable communication among authorized stakeholders. A decentralized architecture incorporating permissioned blockchain and edge computing can address several of these requirements simultaneously.

Therefore, this research proposes a **Secure and Decentralized Health Data Management**

Framework Using IoMT and Blockchain. The proposed framework combines IoMT devices, edge computing, and Hyperledger Fabric to provide secure collection, processing, validation, and controlled exchange of healthcare information. IoMT devices collect patient-related information, while edge nodes perform preliminary processing close to the data source. Relevant transaction information is subsequently recorded through a permissioned blockchain network, providing tamper-resistant records and controlled access for authorized healthcare stakeholders.

The proposed architecture is intended to improve healthcare data integrity, privacy, interoperability, and availability while reducing unnecessary communication between IoMT devices and centralized infrastructures. The framework can support applications such as remote patient monitoring, continuous health observation, secure clinical data exchange, preventive healthcare, and timely medical intervention. The overall objective is to establish a decentralized healthcare data-management model capable of supporting secure and efficient IoMT-based healthcare services.

2. Literature Review

2.1 IoMT-Based Healthcare Systems

S. M. R. Islam et al. presented a comprehensive study of the Internet of Things in healthcare and examined how connected medical devices can support healthcare monitoring, information exchange, and intelligent medical services. Their work also identified several challenges associated with IoT-enabled healthcare, including privacy, security, interoperability, data management, and the reliability of connected devices. The study provides an important foundation for research on IoMT because healthcare applications require stronger protection mechanisms than many conventional IoT applications due to the sensitivity of medical information [1].

T. Saba et al. investigated a secure and energy-efficient framework for IoMT-based e-healthcare. Their research addressed the requirement for maintaining healthcare security while considering the limited computational and energy resources of connected medical devices. The study demonstrates that security mechanisms for IoMT should be designed with both protection and resource efficiency in mind. This observation is relevant to the proposed framework because IoMT devices must be capable of collecting and transmitting healthcare information without excessive computational overhead [2].

S. B. Baker, W. Xiang, and I. Atkinson reviewed IoT technologies for smart healthcare and discussed important opportunities and challenges associated with connected medical environments. Their study highlighted issues related to security, interoperability, scalability, communication, and system integration. The authors emphasized that the growing number of connected healthcare devices requires architectures capable of managing heterogeneous devices and large quantities of medical information. These observations support the development of an integrated IoMT architecture incorporating decentralized data management [3].

2.2 Blockchain for Healthcare Data Integrity

F. Jamil et al. developed an IoT-based blockchain integrity management platform for monitoring patient vital signs in smart hospitals. Their work demonstrated how blockchain can be incorporated into healthcare monitoring to maintain trustworthy records of data generated by connected medical devices. The use of blockchain provides a mechanism for recording transactions in a tamper-resistant manner, which can be particularly useful when patient information is exchanged between multiple healthcare entities. Their findings support the use of blockchain as an integrity layer for IoMT-generated medical information [4].

K. P. Satamraju examined the integration of IoT and blockchain technology in healthcare through a proof-of-concept implementation. The research explored the feasibility of combining connected healthcare devices with blockchain-based data management and demonstrated the potential of blockchain to support secure and scalable healthcare applications. The study is relevant to the proposed work because it illustrates how decentralized ledger technology can be incorporated into IoT-based healthcare environments to improve data trust and transaction management [7].

S. Ali et al. investigated the integration of blockchain and explainable artificial intelligence within metaverse-oriented healthcare applications. Their work considered trust, patient-data protection, and explainability in emerging digital healthcare environments. The study indicates that future healthcare systems will increasingly require mechanisms that can provide both secure information management and transparent technological operations. Blockchain can contribute to this requirement by providing auditable records of data-related transactions [9].

2.3 Privacy and Security in IoMT

M. A. Habib et al. investigated privacy protection for medical information in heterogeneous IoMT environments and considered threats originating from internal as well as external sources. Their work highlights that healthcare security cannot be restricted to protecting communication channels alone because authorized participants may also become potential sources of privacy violations. Effective healthcare architectures must therefore incorporate access control, data protection, and monitoring mechanisms capable of controlling how sensitive information is accessed and used [6].

G. Manogaran, N. Chilamkurti, and C.-H. Hsu examined emerging trends, issues, and challenges associated with IoMT and wireless networks. Their study emphasized the growing complexity of healthcare environments created by the integration of medical sensors, communication networks, and intelligent information systems. The authors identified challenges related to security, scalability, interoperability, and reliable communication, indicating the need for integrated architectures capable of supporting the growing requirements of IoMT applications [8].

2.4 Blockchain, Edge Computing, and Distributed Healthcare

R. Sekaran et al. investigated blockchain-based mobile edge computing for IoT automation. Their work explored the combination of distributed ledger technology and edge computing to support IoT applications with improved processing and communication characteristics. Edge computing can reduce the distance between data-generation devices and computational resources, while blockchain can provide transaction integrity and decentralized trust. The combination is particularly relevant to IoMT because healthcare monitoring applications may require rapid processing of continuously generated physiological information [5].

The integration of edge computing into healthcare data management can reduce unnecessary transmission of raw sensor information to remote cloud platforms. Instead, preliminary filtering, aggregation, and analysis can be performed near the IoMT devices. Only relevant information or verified transaction records need to be transmitted to higher-level systems. This architecture can reduce communication overhead and support applications where rapid response is important, such as remote patient monitoring and emergency healthcare services.

2.5 Healthcare Data Processing and Interoperability

A. H. Sannidhanam investigated scalable web-service architectures for healthcare data processing. The study highlights the importance of scalable service infrastructures capable of processing healthcare information across distributed systems. Such approaches are relevant to IoMT environments because connected medical devices can continuously generate heterogeneous data that must be processed and made available to authorized applications. Scalable service-oriented processing can therefore complement blockchain and edge technologies within a broader healthcare data-management architecture [10].

A. H. Sannidhanam and S. Alladi examined cloud-based healthcare CRM systems with an emphasis on improving patient engagement. Their work demonstrates the importance of integrating digital technologies to manage healthcare information and interactions between patients and healthcare providers. Although cloud-based architectures provide useful centralized services, the increasing sensitivity and distribution of healthcare information create a need for stronger decentralized trust and data-integrity mechanisms [11].

2.6 Research Gap

The reviewed literature demonstrates that IoMT provides an effective foundation for continuous healthcare monitoring, while blockchain can improve data integrity, transaction traceability, and decentralized trust. Edge computing can additionally reduce communication latency and processing overhead by moving selected computational operations closer to IoMT devices. However, many existing studies focus primarily on individual aspects such as IoMT monitoring, blockchain integrity, privacy protection, or edge-based processing rather than integrating these technologies into a unified healthcare data-management framework.

The proposed research addresses this gap by combining **IoMT, edge computing, and Hyperledger Fabric** within a permissioned and decentralized healthcare architecture. IoMT devices act as the primary data-generation layer, edge nodes perform near-source processing, and Hyperledger Fabric provides controlled transaction validation and tamper-resistant record management. This combination is intended to provide a balance among **data security, privacy, integrity, interoperability, scalability, and low-latency healthcare processing**.

Unlike a conventional centralized healthcare repository, the proposed architecture distributes trust among authorized participants while maintaining controlled access to healthcare information. Sensitive patient data can be maintained using appropriate protected storage mechanisms, while blockchain transactions can provide verification, access-control records, and audit trails. This design reduces unnecessary exposure of clinical information while maintaining transparency regarding authorized data operations.

Overall, the literature indicates a clear need for secure and decentralized healthcare infrastructures capable of managing the increasing volume of IoMT-generated information. The proposed framework builds upon existing research by bringing together IoMT, permissioned blockchain, and edge computing into a unified architecture aimed at supporting secure health-data management and efficient healthcare services.

Project Description

Blockchain technology provides a distributed mechanism for recording and validating transactions without relying entirely on a central authority. Its combination of cryptographic protection, distributed consensus, traceability, and tamper resistance makes it suitable for applications that require secure and trustworthy data management. In healthcare, blockchain can help maintain verifiable records, monitor access to sensitive information, and enable controlled sharing among patients, healthcare providers, and researchers.

The increasing use of IoT devices in healthcare has created opportunities for continuous patient monitoring. Wearable and connected medical sensors can measure important physiological parameters, including heart rate, body temperature, blood pressure, oxygen saturation, and other health indicators. However, the secure collection, transmission, storage, and sharing of this information remain challenging because healthcare data is highly sensitive and may pass through multiple devices and organizations. These concerns became particularly evident during large-scale health emergencies, where rapid data exchange was necessary while patient confidentiality still had to be protected.

The proposed project addresses these concerns through the integration of IoMT devices with a permissioned blockchain framework. Health data generated by connected sensors is processed through appropriate stages before being securely validated and recorded. Authorized participants can access information according to predefined permissions, while the distributed ledger provides a traceable record of relevant transactions and data operations. This approach can reduce the risk of unauthorized modification and improve accountability throughout the data lifecycle.

A major characteristic of the proposed framework is its patient-centered approach to data access. Patients and healthcare organizations can establish controlled policies regarding who is permitted to view or use specific health information. Smart contracts can support automated enforcement of these rules, including temporary or restricted access for healthcare professionals and researchers. Such mechanisms can improve trust while facilitating legitimate data sharing for treatment and medical research.

Blockchain offers several important features for the proposed healthcare environment. **Decentralization** distributes validation and management functions among authorized network participants, reducing dependence on a single central repository. **Data integrity** helps detect unauthorized changes and supports the preservation of trustworthy records. **Transparency and traceability** provide an auditable history of authorized transactions, while **cryptographic security** and permission-based access help protect sensitive patient information. By combining these properties with IoMT and edge computing, the proposed system aims to establish a secure, efficient, interoperable, and scalable platform for continuous digital healthcare monitoring and management.

Requirements Engineering

The proposed **Secure and Decentralized Health Data Management System Using IoMT and Blockchain** is designed to provide protected, reliable, and transparent management of sensitive healthcare information. The framework combines blockchain technology with IoMT devices, edge computing, AES encryption, SHA-256 hashing, and a MySQL database to support secure data processing and storage. Medical information is encrypted before storage, while cryptographic hashing is used to verify data integrity. Blockchain-based validation provides an auditable and tamper-resistant record of important transactions, and controlled access policies restrict sensitive information to authorized users. The overall system is designed to support scalable, efficient, and policy-based healthcare data management.

Hardware Requirements

The hardware configuration provides the computing resources required for developing, testing, and operating the proposed system. A standard computer system with sufficient processing capacity, memory, storage, and peripheral devices is adequate for implementation and evaluation.

Software Requirements

The software environment consists of the tools and platforms required for application development, database management, deployment, and testing. Java-based web technologies are used to develop the application interface and server-side functionality, while MySQL manages application data. Apache Tomcat provides the execution environment for the web application.

3. Design Engineering

Design engineering defines the structural and functional representation of the proposed healthcare data management system. Unified Modeling Language (UML) concepts can be used to describe the interactions among users, application modules, data repositories, and security mechanisms. The design provides a structured view of how healthcare data is collected, protected, verified, stored, and accessed. It also supports clear documentation of system behavior and communication between the different entities involved in the healthcare ecosystem.

System Architecture

International Journal of Artificial Intelligence and Computer Electronics
Volume: 02, Issue: 03, July-September 2026, pp:114-124
P-ISSN 3117-8529 | E-ISSN 3117-8537

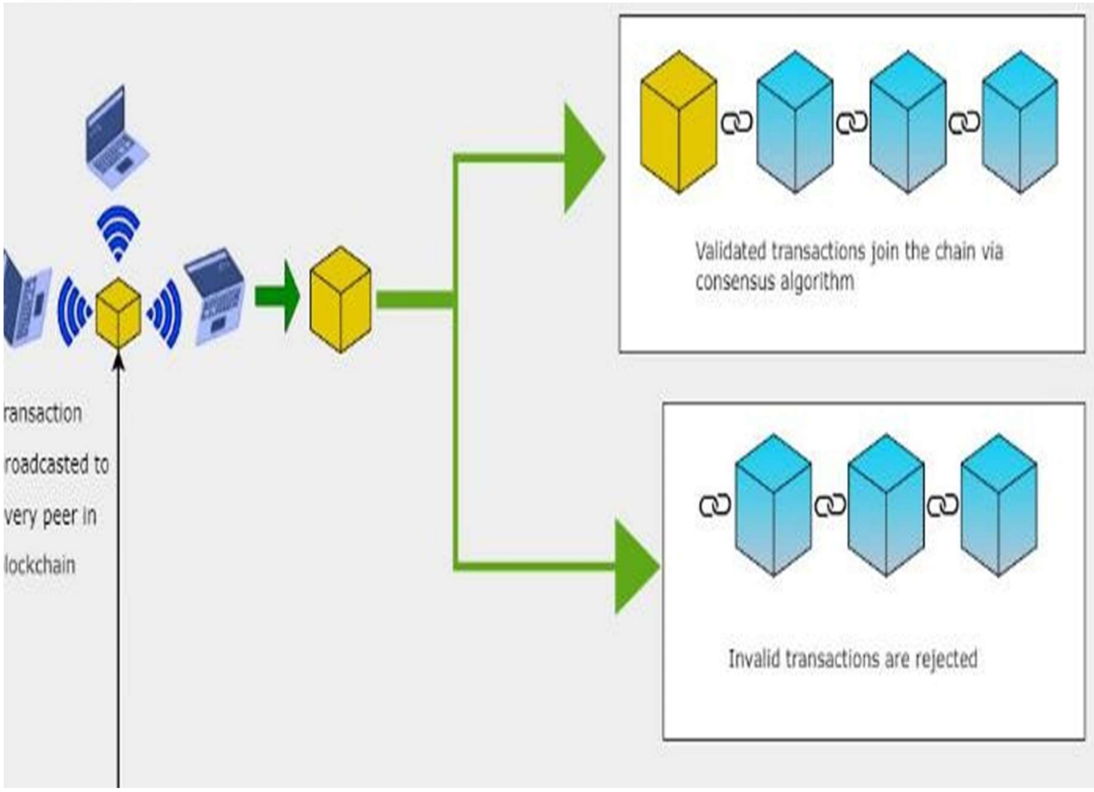

Fig ; 1 System Architecture

The proposed architecture establishes a secure and decentralized healthcare environment by integrating IoMT devices, blockchain technology, AES encryption, SHA-256 hashing, edge computing, and database services. The primary participants in the system are the **Administrator, Hospital, Doctor, and Patient**. The administrator manages user registration and authorization, while hospitals coordinate healthcare services and handle requests from doctors and patients. Patients can register with healthcare institutions and upload their medical records through the application.

Before sensitive medical files are stored or shared, the system encrypts the information using AES encryption. A cryptographic hash generated using SHA-256 is associated with the data to support integrity verification and help identify unauthorized modifications. Relevant transaction information and encrypted data references can then be recorded through the blockchain layer, creating a traceable and tamper-resistant history of data operations.

Doctors who receive appropriate authorization can access verified patient information and use the permitted decryption mechanism to view protected records. They can also provide medical observations or prescriptions through the secure application environment. Edge computing supports the architecture by processing selected IoMT data closer to its source, reducing communication delays and improving responsiveness for real-time healthcare services.

4. Implementation

The proposed secure healthcare data management system is implemented as a Java-based web application that supports controlled interaction among administrators, hospitals, doctors, and patients. The implementation uses Java Servlets and JSP for application processing and user interaction, while MySQL is used to maintain user details, hospital information, requests, and other application records. The system incorporates security-oriented mechanisms for protecting sensitive healthcare information and supports controlled access to medical services and records.

The patient file upload module is designed to handle medical documents submitted through the web application. The implementation is configured to support multipart requests, allowing users to upload files securely. In the complete security workflow, sensitive information can be encrypted before storage, while cryptographic verification can be used to check the integrity of protected healthcare data.

The administrator login module provides restricted access to administrative functions. User credentials are validated before the administrator is redirected to the authorized dashboard. This module acts as an entry point for administrative operations, including the management and approval of healthcare-related entities within the system.

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE AND COMPUTER ELECTRONICS
International Journal of Artificial Intelligence and Computer Electronics
Volume: 02, Issue: 03, July-September 2026, pp:114-124
P-ISSN 3117-8529 | E-ISSN 3117-8537

The doctor–hospital association module enables registered doctors to submit requests to join a selected hospital. The system retrieves the doctor's registered information from the database and creates a hospital request containing relevant professional details. Each request is assigned an identifier and stored with a pending status until it is processed by the appropriate healthcare authority. This mechanism provides a structured workflow for establishing doctor–hospital associations.

Similarly, the patient–hospital association module allows patients to submit requests to healthcare institutions. Patient information is retrieved from the registered database record and included in the request sent to the selected hospital. The request remains in a pending state until approval or further action is taken. This process helps organize patient enrollment and facilitates controlled access to hospital services.

The system also includes an email-based One-Time Password (OTP) utility for supporting user verification. The module generates and sends an OTP to the registered email address through an SMTP-based communication service. OTP verification provides an additional authentication mechanism and can help reduce unauthorized access during sensitive operations. For deployment in a production environment, email credentials and other security secrets should be stored securely outside the application source code.

5. Results

The proposed system is implemented as a web-based healthcare management application that provides separate interfaces for different categories of users. The application is developed using Java-based web technologies, including Core Java, JSP, and Servlets, while database operations are handled through MySQL. Cascading Style Sheets are used to improve the presentation and usability of the user interface. The snapshots presented in this chapter illustrate the main functional screens and the interaction flow of the proposed application.

Home Page

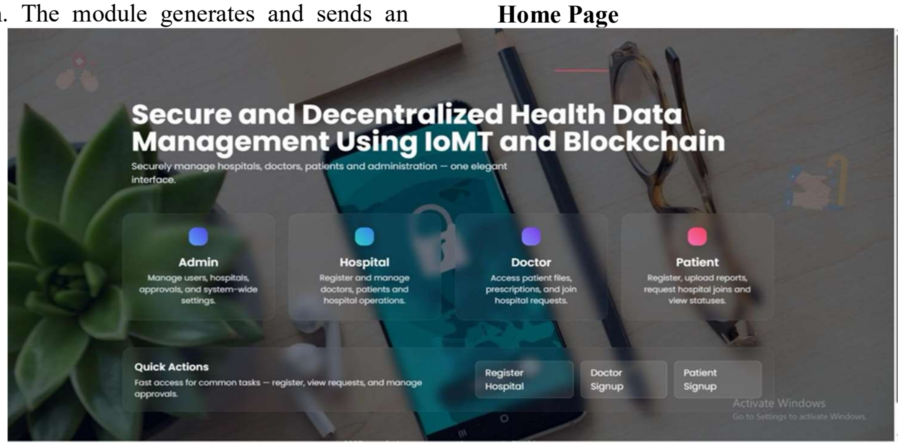

Fig ; 2

The home page serves as the initial interface of the application and provides users with access to the available system functions. It acts as the entry point through which administrators, patients, doctors, and other authorized users can navigate to the appropriate modules.

Admin login

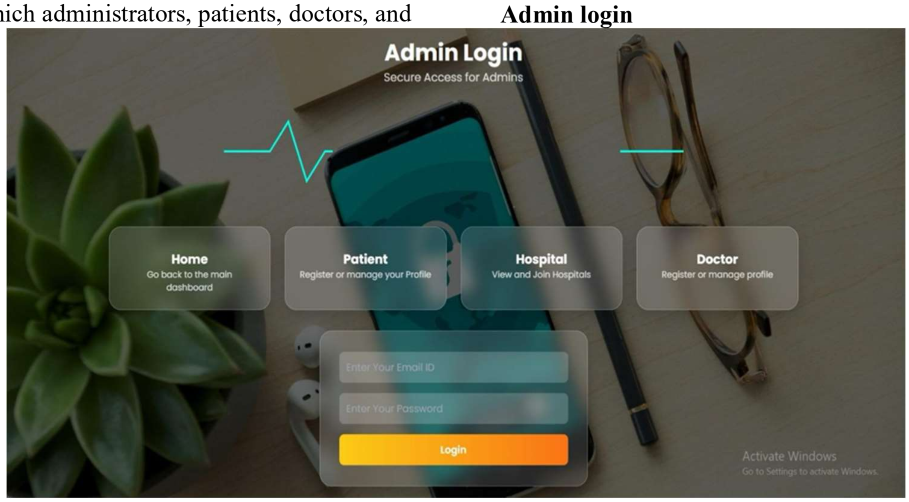

Fig ; 3

International Journal of Artificial Intelligence and Computer Electronics
Volume: 02, Issue: 03, July-September 2026, pp:114-124
P-ISSN 3117-8529 | E-ISSN 3117-8537

The Administrator Login Page Provides Secure Access To The Administrative Section Of The System. After Successful Authentication, The Administrator Can Access Authorized Functions Related To System Management, User Monitoring, And The Coordination Of Healthcare Entities.

Patient Registration

Fig ; 4

The patient registration page enables new patients to create an account by submitting the required personal and contact information. The registration process establishes a patient profile that can subsequently be used for authentication, hospital association, healthcare record management, and other authorized services.

Doctor Registration

Fig ; 5

The doctor registration interface allows healthcare professionals to register their details within the application. Information such as professional identity, specialization, designation, contact details, and other required fields can be maintained in the system to support hospital association and patient care activities.

Patient Registration Request

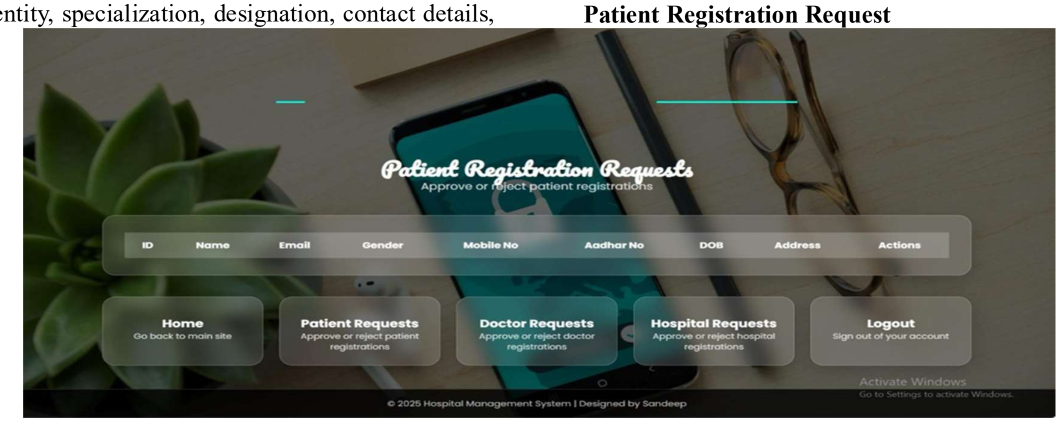

Fig ; 6

The patient request module enables healthcare-related requests to be submitted and reviewed through a structured workflow. Request information is maintained with an appropriate status, allowing the relevant authority or institution to process pending applications in an organized manner.

Patient Join Hospital

International Journal of Artificial Intelligence and Computer Electronics
Volume: 02, Issue: 03, July-September 2026, pp:114-124
P-ISSN 3117-8529 | E-ISSN 3117-8537

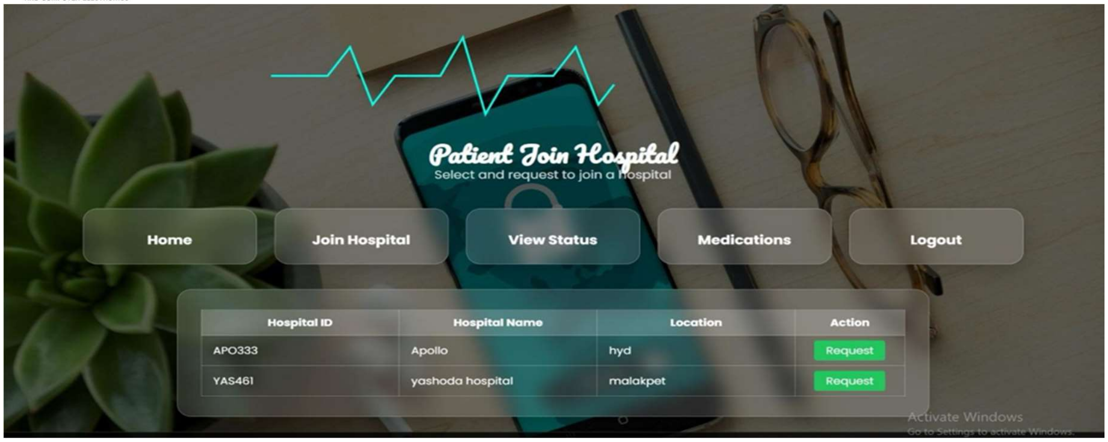

Fig ; 7

The patient–hospital association page allows registered patients to request enrollment with a selected healthcare institution. The submitted request is stored for review, and the patient can subsequently receive information about the status of the request.

Patient View Status

Fig ; 8

The patient status page enables users to monitor the progress of their submitted hospital or registration requests. This feature improves transparency by allowing patients to determine whether their requests remain pending, have been approved, or require further action.

Software Testing

Software testing is performed to verify that the developed application operates according to its specified functional and security requirements. The objective is to identify defects, incorrect behavior, integration problems, and other weaknesses before the system is deployed for practical use. Testing evaluates individual modules as well as the overall interaction among components to ensure that the application provides reliable services and handles user operations appropriately.

For the proposed healthcare management system, testing focuses on important functions such as user registration, login authentication, session management, doctor and patient hospital requests, database communication, request-status processing, file handling, and email-based OTP functionality. These tests help determine whether valid user inputs produce the expected results and whether invalid or unauthorized operations are handled safely.

Testing Methodology

The testing process begins with the preparation of a test plan based on the functional requirements of the application. Individual modules are first evaluated to verify their independent behavior, followed by integration testing to examine communication among the web interface, server-side application, database, and authentication components. System-level testing is then used to assess the complete workflow under normal operating conditions.

Functional testing verifies that each feature performs its intended task, while input validation testing checks the system's response to incorrect or incomplete information. Authentication and authorization testing are used to confirm that

International Journal of Artificial Intelligence and Computer Electronics
Volume: 02, Issue: 03, July-September 2026, pp:114-124
P-ISSN 3117-8529 | E-ISSN 3117-8537

protected functions are available only to permitted users. Database testing verifies the correct insertion, retrieval, and updating of records, whereas integration testing examines the flow of information between connected modules.

The application can also be evaluated across supported browsers and different system configurations to identify compatibility issues. Errors identified during testing are corrected and the affected functions are retested. This iterative process improves the stability and reliability of the proposed system and helps ensure that the final application meets its expected operational requirements.

Future Enhancements

The proposed blockchain-enabled IoMT healthcare framework can be further extended through the integration of Artificial Intelligence and Machine Learning techniques for intelligent analysis of continuously generated patient data. Such capabilities could support early disease identification, risk assessment, anomaly detection, and personalized treatment recommendations. Future versions may also incorporate federated learning, allowing multiple healthcare organizations to collaboratively develop analytical models without transferring sensitive patient data to a centralized repository. Privacy-preserving technologies, including zero-knowledge proofs and homomorphic encryption, could further strengthen secure information sharing among hospitals and other authorized stakeholders.

The framework may also be enhanced through advanced smart contracts that automate approval, verification, and access-control processes. A cloud-edge collaborative architecture could improve scalability and reduce response time for continuous monitoring applications. In addition, interoperability mechanisms may enable secure data exchange among healthcare institutions across different regions or countries. Developing a mobile-based decentralized healthcare application would further improve accessibility and allow patients, doctors, and hospitals to interact with the system more conveniently. These enhancements could support the development of a more intelligent, scalable, interoperable, and patient-centered IoMT healthcare ecosystem.

Conclusion

The proposed blockchain-enabled IoMT healthcare system presents a secure and decentralized approach for managing sensitive medical information among patients, doctors, hospitals, and authorized administrators. The framework combines IoMT-based data collection with AES encryption to protect confidentiality and SHA-256 hashing to support data integrity verification. Blockchain technology provides a traceable and tamper-resistant mechanism for recording relevant data transactions, thereby improving transparency and accountability within the healthcare environment.

The system implements controlled user access through authentication and administrative approval mechanisms. Hospital, doctor, and patient modules support organized healthcare interactions and controlled sharing of medical information. Patients can manage and share their records with authorized healthcare professionals, while doctors can access permitted information for clinical activities. The use of edge computing further supports faster processing of data generated by connected medical devices and can reduce delays in real-time monitoring scenarios.

Reference

1. S. M. R. Islam, D. Kwak, M. D. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for healthcare: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.
2. T. Saba, K. Haseeb, I. Ahmed, and A. Rehman, "Secure and energy-efficient framework using the Internet of Medical Things for e-healthcare," *Journal of Infection and Public Health*, vol. 13, no. 10, pp. 1567–1575, 2020.
3. S. B. Baker, W. Xiang, and I. Atkinson, "Internet of Things for smart healthcare: Technologies, challenges, and opportunities," *IEEE Access*, vol. 5, pp. 26521–26544, 2017.
4. Sannidhanam, A. H. (2025). Autonomous AI Agents for Cloud Infrastructure Operations. *Journal of Contemporary Science and Technology Management, 1*(01), 83–100.
5. L.K.Suresh Kumar , Mohammed Abdul Bari , "*Zero-Day Attack Detection In Multi-Tenant Cloud Environments Using Variational Autoencoder*s ," International Journal of Applied Mathematics, ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)Volume 38 No. 3s, 2025.
6. Anjani Haritha Sannidhanam. (2024). Guardrails and Safety Mechanisms for LLM-Powered Enterprise Applications. *International Journal of Engineering Science & Humanities, 14*(3), 273–285.
7. F. Jamil, S. Ahmad, N. Iqbal, and D.-H. Kim, "Remote monitoring of patient vital signs using an IoT-based blockchain integrity management platform in smart hospitals," *Sensors*, vol. 20, no. 8, p. 2195, 2020.

8. R. Sekaran, R. Patan, A. Raveendran, F. Al-Turjman, M. Ramachandran, and L. Mostarda, "Blockchain-based 6G-enabled mobile edge computing for IoT automation," *IEEE Access*, vol. 8, pp. 143453–143463, 2020.
9. Sannidhanam, A. H. (2020). Scalable Web Services Architecture for Healthcare Data Processing. *International Journal of Recent Advances in Science and Technology, 7*(01), 1–14.
10. Event Streaming Architectures for High-Volume Transaction Processing. (2022). *International Journal of Advance Industrial Engineering, 10*(01), 1–8. doi:10.14741/
11. M. A. Habib et al., "Privacy-based medical data protection against internal security threats in heterogeneous Internet of Medical Things," *International Journal of Distributed Sensor Networks*, vol. 15, no. 9, 2019.
12. K. P. Satamraju, "Scalable integration of Internet of Things and blockchain technology in healthcare: A proof-of-concept," *Sensors*, vol. 20, no. 5, p. 1389, 2020.
13. Vishwanath Nikhil , Dr. Mohammed Abdul Bari *," Real Time Powerlifting Form Assessment using Yolov5 and Mediapipe*", International Journal of Information Technology and Computer Engineering, SSN 2347–3657, Volume 13, Special Issue 2s, 2025, Pages 574-584
14. G. Manogaran, N. Chilamkurti, and C.-H. Hsu, "Emerging trends, issues, and challenges in the Internet of Medical Things and wireless networks," *Personal and Ubiquitous Computing*, vol. 22, nos. 5–6, pp. 879–882, 2018.
15. Sannidhanam, A. H. (2020). Scalable Web Services Architecture for Healthcare Data Processing. *International Journal of Recent Advances in Science and Technology, 7*(01), 1–14.
16. Shaik Abdul Waheed, Mohammed Sulaiman, Mirza Awaiz Baig, Dr. Mohammed Abdul Bari," *Intelligent Conversational Agent for Seamless User Interaction Using NLP and Dialog flow*",International Journal of Information Technology and Computer Engineering, SSN 2347–3657 ,Volume 13, Special Issue 2s, 2025, Page -91-98.
17. S. Ali et al., "Metaverse in healthcare integrated with explainable AI and blockchain: Enabling immersiveness, ensuring trust, and protecting patient data," *Sensors*, vol. 23, no. 2, p. 565, 2023.
18. A. J. Lafta, A. F. Mahmood, and B. M. Saeed, "5G and Internet of Things: Next-generation network architecture," *Journal of Information and Communication Convergence Engineering*, vol. 22, no. 3, pp. 189–198, 2024.
19. Sannidhanam, A. H., & Alladi, S. (2017). Cloud-Based Healthcare CRM Systems for Improved Patient Engagement. *International Journal of Technology, Management and Humanities, 3*(01), 32–44. doi:10.21590/ijtmh.3.03.4
20. Distributed Data Processing Frameworks for Large-Scale Healthcare Analytics. (2019). *International Journal of Advance Industrial Engineering, 7*(04), 1–10. doi:10.14741/ijaie/v.7.4.01
21. Anjani Haritha Sannidhanam. (2023). Self-Healing Distributed Systems: AI-Driven Failure Prediction and Automated Recovery. *International Journal of Research & Technology, 11*(4), 168–174.
22. Sannidhanam, A. H. (2025). Autonomous AI Agents for Cloud Infrastructure Operations. *Journal of Contemporary Science and Technology Management, 1*(01), 83–100.
23. Event Streaming Architectures for High-Volume Transaction Processing. (2022). *International Journal of Advance Industrial Engineering, 10*(01), 1–8. doi:10.14741/

About Author

Mohd Wasif Ur Rahman is currently pursuing a Master of Technology in Computer Science and Engineering at ISL Engineering College, affiliated with Osmania University, Hyderabad, India. He completed his Bachelor of Engineering in Information Technology from ISL Engineering College, affiliated with Osmania University, from 2019 to 2023.