IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN:2349-2163
Volume 13, Issue 04, April https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2026.v1304.07

Secure & Decentralized Health Data Management Using IoMT and Blockchain

K.Vigneshwar
Assistant Professor, Department of CSE
Guru Nanak Institute of Technology, Hyderabad
kvigneshwar.gnit@gniindia.org
https://orcid.org/0009-0003-9552-1107
P.Shreshta, N.Harshini, S.Saipriya
UG Student, Department of CSE
Guru Nanak Institute of Technology, Hyderabad
shreshtapuppala5@gmail.com , neelamharshini02@gmail.com , sabbireddysaipriya26@gmail.com

Publication History
Manuscript Reference No: IJIRAE/RS/Vol.13/Issue04/AEAP26.APAE10086
Research Article | Open Access | Double-Blind Peer-Reviewed| Article ID: IJIRAE/RS/Vol.13/Issue04/AEAP26.APAE10186
Received:02,March 2026, Revised: 29, March 2026, Accepted: 10,April 2026,Published Online: 22, April 2026.
https://www.ijirae.com/volumes/Vol13/iss-04/07.AEAP26.APAE10086.pdf
Article Citation: Vigneshwar,Shreshta,Harshini,Saipriya(2026),Secure & Decentralized Health Data Management Using IoMT and Blockchain,IJIRAE: International Journal of Innovative Research in Advanced Engineering, Volume 13, Issue 04 of 2026 pages 772-778 **Doi:>** https://doi.org/10.26562/ijirae.2026.v1304.07
BibTeX Key: Vigneshwar@2026Secure
IJIRAE papers should be cited as IJIRAE (International Journal of Innovative Research in Advanced Engineering, AM Publications, India 2025, ISSN 2349-2163, https://doi.org/10.26562/ijirae.2026.v1304.07 The journal's official abbreviation is IJIRAE. Orcid: https://orcid.org/0009-0004-9398-7488 About the License: Copyright©2026 copyright by the authors. This article is an open access and license under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

Abstract: The rapid advancement and integration of Internet of Medical Things (IoMT) devices are reshaping modern healthcare by enabling real-time patient monitoring, early diagnosis, and intelligent clinical decision-making. However, a key challenge persists in the fragmentation of sensitive patient data across healthcare institutions, limiting interoperability and raising privacy concerns. To address this, the project proposes a blockchain-enabled framework using Hyperledger Fabric to ensure secure, tamper-resistant, and privacy-preserving data storage with robust access control and auditability. Additionally, edge computing is integrated to process data closer to the source, reducing latency and improving efficiency. This decentralized architecture enables secure, real-time data sharing while maintaining data integrity and confidentiality.
Keywords:-Internet of Medical Things (IoMT), Blockchain Technology, Hyperledger Fabric, Healthcare Data Security, Decentralized Systems, Edge Computing, Secure Data Sharing, Interoperability

I. INTRODUCTION

The Internet of Things (IoT) has emerged due to the increasing number of connected devices, significantly improving healthcare through the Internet of Medical Things (IoMT). IoMT systems consist of wearable sensing devices connected via a wireless body area network (WBAN), an internet gateway, and a cloud-based data center, generating personal health data such as heart rate, and blood sugar levels for local or cloud-based analysis. The digitization of patient records supports remote monitoring, timely decision-making, and advanced medical research, enhancing overall healthcare efficiency and patient outcomes; however, fragmented data storage, unstable network infrastructure, and the massive volume of generated data hinder efficient data exchange and accessibility, while critical concerns such as data privacy regulations, increased risk of security breaches, and communication disruptions under abnormal conditions further complicate IoMT implementation. The proposed framework integrates IoMT and blockchain[18] for the secure recording, processing, and storage of health metrics is preprocessed and securely stored in the blockchain to ensure tamper-proof records and transparency, while also enabling real-time access, visualization, and continuous monitoring of patient health, supporting proactive healthcare management, early diagnosis, and delivering a robust, decentralized, and scalable solution for secure, reliable, and efficient healthcare data management.

A. Objective

The main goal of this project is to design and implement a secure, interoperable, and privacy-preserving framework for managing data generated by the Internet of Medical Things (IoMT). This project focuses on developing a blockchain-enabled architecture using Hyperledger Fabric to ensure the secure, tamper-proof, and transparent storage and validation of IoMT data. By leveraging blockchain technology, the framework aims to enhance interoperability among diverse healthcare systems, enabling seamless and trustworthy data sharing across multiple institutions while maintaining data integrity. Additionally, the integration of edge computing allows data processing to occur closer to IoMT devices, significantly reducing latency and improving the overall efficiency of the system. The framework also emphasizes robust access control and privacy protection through a permissioned blockchain architecture specifically designed to meet healthcare security and compliance requirements.

B. Problem Statement

The rapid adoption of the Internet of Medical Things (IoMT) has enabled continuous monitoring and real-time collection of patient health data through interconnected medical devices such as wearable sensors, smart implants, and remote monitoring systems. However, this increasing volume of sensitive health data introduces significant challenges related to data security**,** privacy**,** integrity**,** and centralized control. Traditional healthcare data management systems rely heavily on centralized architectures, which are vulnerable to data breaches, unauthorized access, single points of failure, and lack of transparency. Patients often have limited control over their own medical data, and sharing information across different healthcare providers can be inefficient, insecure, and prone to inconsistencies.

C. Scope of the Project

The project "Secure and Decentralized Health Data Management using IoMT and Blockchain" focuses on designing and implementing a system that ensures secure, transparent, and efficient handling of healthcare data generated from IoMT devices. This project primarily covers the integration of IoMT-based data collection with blockchain technology to create a decentralized platform for managing patient health records. It includes the development of mechanisms for secure data transmission, encryption, and access control, ensuring that only authorized entities such as doctors, patients, and healthcare providers can access sensitive information[17,19].

II. LITERATURE SURVEY

A.A.Khanetal [1] (2025) presented a lightweight authentication framework integrating blockchain and edge computing for IoMT environments. The system uses permissioned blockchain networks (similar to Hyperledger) to ensure secure and fast authentication. Edge computing reduces latency by processing data near IoMT devices, enabling faster response times for real-time healthcare applications.

R. Arul, Y. D. Al-Otaibi [2] (2024) proposed an "Multi-Modal Secure Healthcare Data Dissemination Framework Using Block chain in IoMT" aims to develop a secure, transparent, and efficient system for managing and sharing healthcare data collected from diverse Internet of Medical Things (IoMT) devices. In modern healthcare environments, vast amounts of multi-modal data- such as medical images, sensor readings, and patient records- are generated continuously, requiring robust mechanisms for secure storage, validation, and dissemination. This project leverages block chain technology to ensure data integrity, traceability, and tamper-proof management, enabling trusted collaboration among healthcare providers, patients, and researchers.

M. Qi,Z. Wang [3] (2024) introduced blockchain and distributed ledger technologies can be integrated with internet-of-healthcare-things (IoHT) systems to protect privacy. It identifies key privacy challenges (such as meaningful consent, data profiling, lack of trust) in IoHT systems and reviews blockchain-based privacy-preserving techniques (access control, authentication, encryption, federated learning, multi-party computation)

A.J.Lafta, [4] (2024) introduced the "5G and Internet of Things: Next-Gen Network Architecture" focuses on developing a high-speed, low-latency, and intelligent communication framework that integrates the power of 5G technology with the Internet of Things (IoT). With billions of interconnected devices emerging across industries, the project aims to design an architecture that ensures seamless connectivity, real-time data processing, and efficient resource utilization..

M.Khan,S.Ahmed,andL.Wang [5] (2024) presented an edge-enabled blockchain architecture to improve the security and performance of healthcare data management in IoMT systems. The framework combines edge computing with blockchain to process medical data closer to the source, thereby reducing latency and bandwidth consumption. Blockchain ensures data immutability and transparency, while edge nodes handle real-time data filtering and encryption.

S. Ali, Abdullah. [6] (2023) developed "Metaverse in Healthcare Integrated with Explainable AI and Block chain: Enabling Immersiveness, Ensuring Trust, and Providing Patient Data Security" focuses on creating a virtual, intelligent, and secure healthcare ecosystem that combines the immersive power of the Metaverse with the transparency of block chain and the intelligence of explainable AI (XAI). This framework enables virtual medical consultations, remote surgeries, and interactive therapy sessions through immersive 3D environments, enhancing patient engagement and accessibility.

III. SYSTEM DESIGN

A. System Architecture

The system architecture for Secure and Decentralized Health Data Management using IoMT and Blockchain integrates Internet of Medical Things (IoMT) devices, cloud storage, and blockchain technology to ensure privacy, security, and integrity of patient data. IoMT devices collect real-time health data from patients, which is encrypted and stored in a distributed ledger using blockchain.

B. Methodology

The proposed methodology for the project "Secure and Decentralized Health Data Management Using IoMT and Blockchain" is designed as a layered system that ensures secure, controlled, and efficient management of healthcare data. Instead of real-time IoMT devices, the system currently collects patient medical data through text-based files and email inputs, which act as digital representations of patient health records. These records are uploaded by patients and stored securely in the system. At the initial stage, users such as Admin, Hospital, Doctor, and Patient interact with the system through a web-based interface. The system implements role-based access control, where each user is authenticated using OTP-based verification[7,8].

C. Modules

1) Block Chain: The Block chain module forms the core security layer of the proposed healthcare system. It provides a decentralized, immutable, and transparent ledger for storing encrypted patient data and system transactions

2) Edge Computing: The Edge Computing module is integrated to ensure low latency, fast data processing, and efficient resource utilization in healthcare environments. Instead of sending all medical data to centralized cloud servers, computations are performed at the network's edge closer to IoMT devices such as sensors, wearables, and hospital monitoring systems.

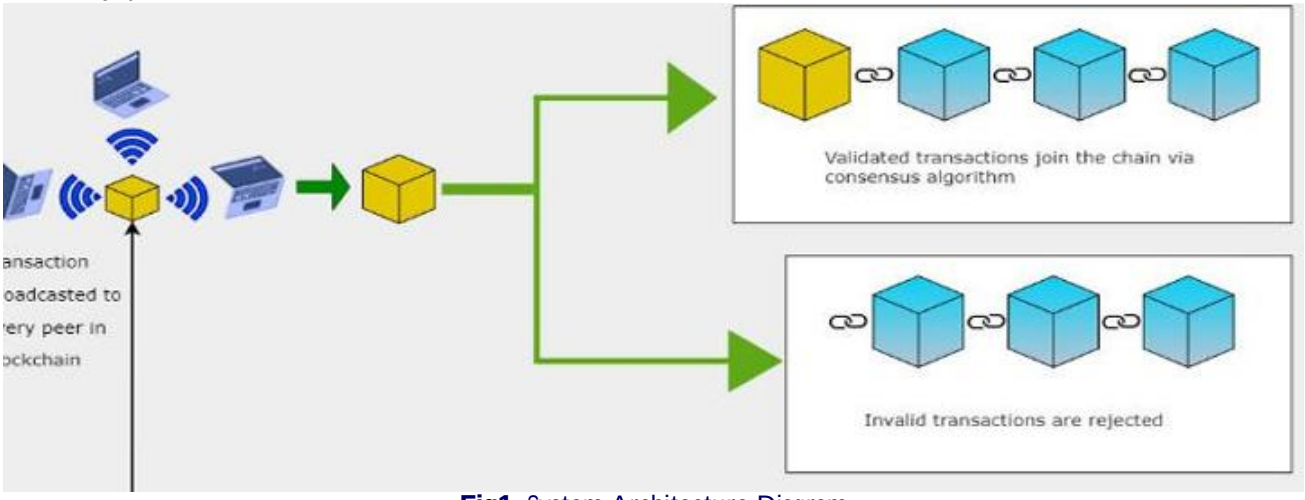

Fig1: System Architecture Diagram

3) AES: The AES module is implemented to achieve strong data encryption of medical files uploaded by patients. AES, a symmetric key encryption algorithm, ensures that patient records are converted into secure cipher text before being stored or transmitted. Only authorized users possessing the secret key can decrypt and access the data [12,13,14].

4) SHA-256: The SHA-256 (Secure Hash Algorithm 256-bit) module is responsible for generating a unique hash value for each uploaded medical file. This hash acts as adigital fingerprint, ensuring data integrity by verifying that the file has not been altered or tampered with. Even a minor modification in the file changes the hash value entirely, making unauthorized changes immediately detectable.

5) JSP Dashboard: Displays the uploaded encrypted data along with file details and timestamps. It also shows the transaction status, verification results, pending registration details, and overall project modules. The dashboard acts as the user interface for monitoring stored data, status, and user details etc

6) MySQL Database: The MySQL database is used to maintain user details, device metadata, and other non-critical information that supports the system's operation.

IV. EXISTING SYSTEM VS PROPOSED SYSTEM

A. Existing System

The Existing proprietary platforms to manage and store medical data, often leading to fragmentation and lack of interoperability between various healthcare providers and devices. In traditional systems, sensitive patient information is often stored in silos across different healthcare organizations, making it difficult for healthcare providers to access ac comprehensive view of a patient's health. While Internet of Medical Things (IoMT) devices have been integrated into healthcare settings to enable real-time monitoring and data collection, the data generated from these devices is not always easily shared or accessible across various platforms. These devices may be connected to different networks, and the data they generate is typically stored in isolated systems, limiting its utility for healthcare professionals who need a broader, unified view of patient health[9,10,11]. Traditional healthcare data storage systems often use centralized databases, which are vulnerable to cyber-attacks and unauthorized access.

B. Proposed System.

The proposed system introduces a secure, decentralized, and efficient healthcare data management framework that integrates Internet of Medical Things (IoMT) devices with block chain technology and edge computing to overcome the limitations of traditional centralized systems. This architecture uses hyper ledger Fabric, a permissioned block chain network, to securely store and manage sensitive health data, ensuring data privacy, and immutability. The use of edge computing enhances real-time data processing and enables timely clinical responses, while block chain ensures that all health records are tamper-proof and transparently auditable[15,16].

V. IMPLEMENTATION

A. Environment Initalization

Configured an Apache Tomcat server to deploy and manage the application efficiently. Established a MySQL database connection using JDBC to handle data operations securely and reliably. Set up the development environment by installing Java, an IDE such as Eclipse or IntelliJ, and all required libraries. Integrated SMTP services to enable secure OTP-based email verification. Ensured all components worked together smoothly to support application functionality.

B. System Workflow Execution

The system supports user registration with an admin approval process to ensure authorized access. It provides secure login functionality using OTP-based authentication for enhanced security. Patients can upload their medical records in text format for further review. Hospitals access these records using a unique secret key to maintain data privacy.

Based on the patient's condition, hospitals assign doctors for detailed analysis. Doctors then examine the records and provide appropriate prescriptions. Finally, patients can view their prescriptions through a personalized dashboard for easy access and tracking.

VI. RESULTS AND DISCUSSION

This section features screenshots that provide visual documentation of the system development, functionality and user interface evidence. The snapshots provide a clear representation of how the application works in real-time, and illustrates main functionality during release.

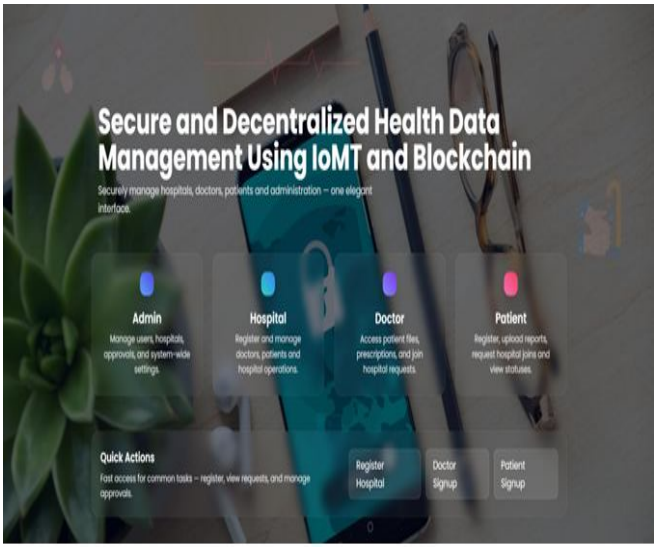

Fig: Home Page

Fig: Admin Page

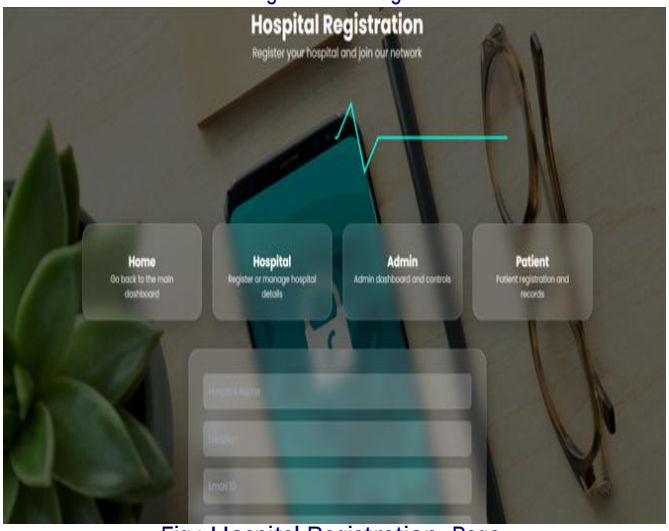

Fig.: Hospital Registration Page

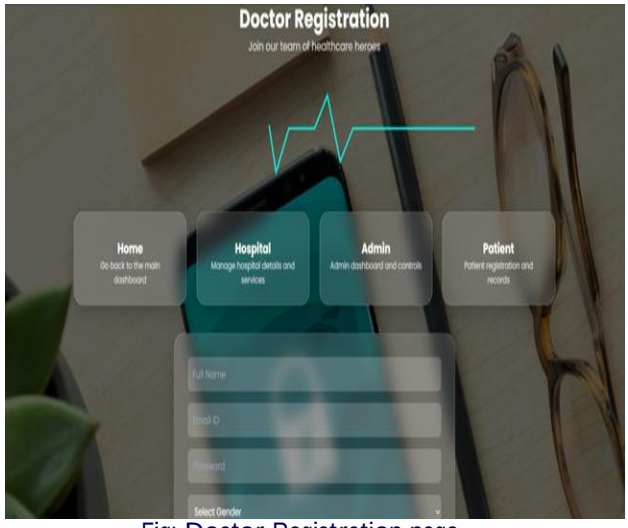

Fig: Doctor Registration page

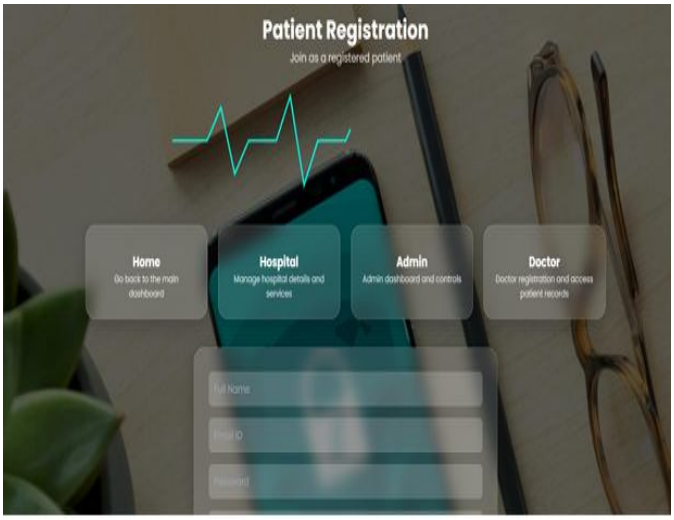

Fig: Patient Registration page

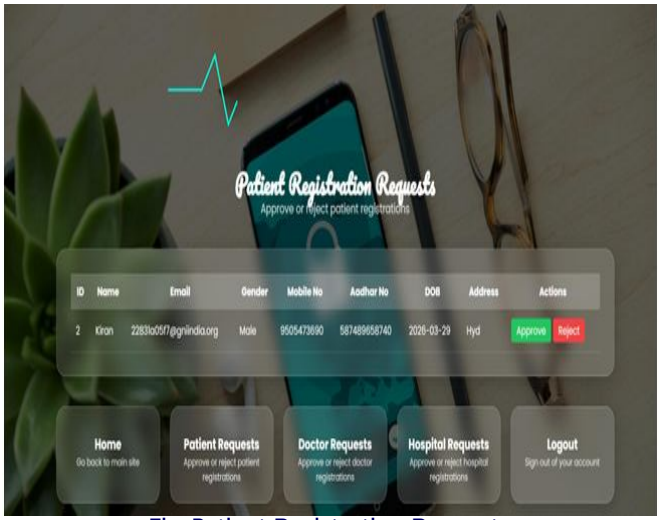

Fig: Patient Registration Request

Fig: Upload files

This module allows patients to upload their medical documents in text file format. The uploaded files are securely stored in the system and can be accessed later by the hospital for review

Fig: Allocation page

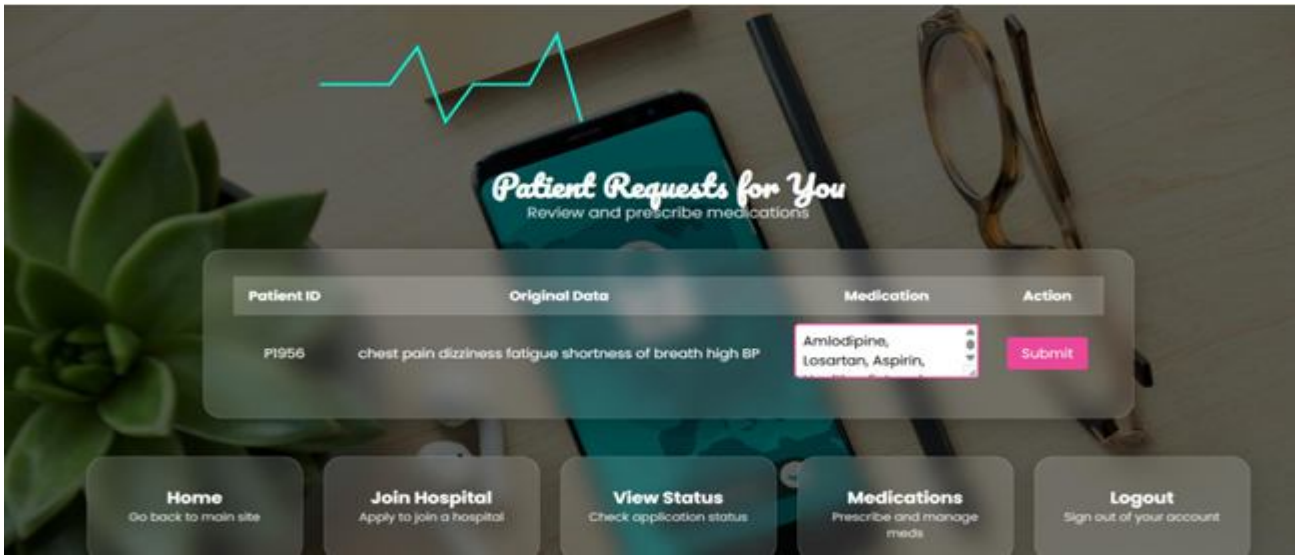

Fig: Patient Request page

Once a doctor is assigned, they can access the patient's medical records uploaded in the system. Based on the data, the doctor analyzes the condition and prescribes appropriate medications.

Fig : view medication page

Patients can view the medications prescribed by the doctor on their dashboard. This ensures they have easy access to treatment details and follow the prescribed care plan

VII. CONCLUSION

In conclusion, the proposed Block chain-enabled IoMT healthcare system successfully establishes a secure, transparent, and decentralized platform for managing sensitive medical data among patients, doctors, and hospitals. By integrating AES encryption for data confidentiality and SHA-256 hashing for integrity verification, the system ensures that patient records remain protected from unauthorized access and tampering. The use of Block chain technology provides immutability and traceability, making every medical transaction verifiable and trustworthy. Through the Admin-controlled approval mechanism, only authenticated users gain access, enhancing overall data governance. The Hospital module streamlines patient–doctor interactions, while the Doctor module allows secure viewing and updating of medical details using secret keys. The Patient module empowers individuals to control their medical data and securely share it with healthcare professionals. With edge computing integration, the system achieves low latency processing and real-time data handling from IoMT devices.

ACKNOWLEDGMENT

The authors express sincere gratitude to Mr.K.Vigneshwar, Assistant Professor, CSE Department, for her valuable guidance and continuous support. They also thank Dr.B.Santhosh Kumar, Head of the Department, for expert supervision, and the faculty members and lab technicians of the CSE Department, Guru Nanak Institute of Technology, Hyderabad, for their assistance and cooperation throughout this project.

REFERENCES

1. S.M.R.Islam, D.Kwak, M.D.H.Kabir, M.Hossain, and K.S.Kwak, “The Internet of Things for health care: 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 Internet of Medical Things for e-healthcare,” J. Infection Public Health, vol. 13, no. 10, pp. 1567–1575, Oct. 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. F.Jamil, S.Ahmad, N.Iqbal, and D.H.Kim, “Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals,” Sensors, vol. 20, no. 8, p. 2195, Apr. 2020.
5. R.Sekaran, R.Patan, A.Raveendran, F.Al-Turjman, M.Ramachandran, and L.Mostarda, “Survival study on blockchain based 6G-enabled mobile edge computation for IoT automation,” IEEE Access, vol. 8, pp. 143453–143463, 2020.
6. M.A.Habib, C.M.N.Faisal, S.Sarwar, M.A.Latif, F.Aadil, M.Ahmad, R. Ashraf, and M. Maqsood, “Privacy-based medical data protection against internal security threats in heterogeneous Internet of Medical Things,” Int. J. Distrib. Sensor Netw., vol. 15, no. 9, Sep. 2019, Art. no. 155014771987565.
7. K.P.Satamraju, “Proof of concept of scalable integration of Internet of Things and blockchain in healthcare,”Sensors, vol. 20, no. 5, p. 1389, Mar. 2020.
8. G.Manogaran, N.Chilamkurti, and C.-H. Hsu,“Emerging trends, issues, and challenges in Internet of Medical Things and wireless networks,” Pers. Ubiquitous Comput., vol. 22, nos. 5–6, pp. 879–882, Oct. 2018.
9. S.Ali, Abdullah, T.P.T.Armand, A.Athar, A.Hussain, M. Ali, M. Yaseen, M.-I. Joo, and H.-C. Kim, “Metaverse in healthcare integrated with explainable AI and blockchain: Enabling immersiveness, ensuring trust, and providing patient data security,” Sensors, vol. 23, no. 2, p. 565, Jan. 2023.

10. A.J.Lafta, A.F.Mahmood, and B.M.Saeed, "5G and Internet of Things: Next-gen network architecture," J. Inf. Commun. Converg. Eng., vol. 22, no. 3, pp. 189–198, Sep. 2024.
11. S.F.Ackley, S.Pilewski, V.S.Petrovic, L.Worden, E.Murray, and T.C.Porco, "Assessing the utility of a smart thermometer and mobile application as a surveillance tool for influenza and influenza-like illness," Health Informat. J., vol. 26, no. 3, pp. 2148–2158, Sep. 2020.
12. S.Ahmed, M.Saqib, M.Adil, T.Ali, and A.Ishtiaq, "Integration of cloud computing with Internet of Things and wireless body area network for effective healthcare," in Proc. Int. Symp. Wireless Syst. Netw. (ISWSN), Nov. 2017, pp. 1–6.
13. M.Haghi Kashani, M.Madanipour, M.Nikravan, P.Asghari, and E.Mahdipour, "A systematic review of IoT in healthcare: Applications, techniques, and trends," J. Netw. Comput. Appl., vol. 192, Oct. 2021, Art. no. 103164.
14. J.B.Awotunde, R.G.Jimoh, S.O.Folorunso, A.E.Adeniyi, M.K.Abiodun, and O.Banjo, "Privacy and security concerns in IoT-based healthcare systems," in The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care, Cham, Switzerland: Springer, 2021, pp. 105–134.
15. E.Androulakiet al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," in Proc. 13th EuroSys Conf., Apr. 2018, pp. 1–5.
16. P.Chinnasamy, R.K.Ayyasamy, P.Alagarsundaram, S.Dhanasekaran, B.S.Kumar and A.Kiran, "Blockchain Enabled Privacy- Preserved Secure e-voting System for Smart Cities," 2024 International Conference on Science Technology Engineering and Management (ICSTEM), Coimbatore, India, 2024, pp. 1-6, doi: 10.1109/ICSTEM61137.2024.10560826.
17. Chinnasamy, P., Dhavamani, L., Ayyasamy, R.K. et al. QuantumBlock health records: enhancing healthcare data security with quantum cryptography and blockchain technology. Cluster Comput **28**, 474 (2025). https://doi.org/10.1007/s10586-025-05101-w.
18. P.Chokkamreddy, A.Palagati, A.L.P.Rao, P.Maheswari, V.Mahadevan and S.K.Balan, "Utilizing Blockchain Technology for Financial Services in Parallel, Distributed, and Grid Computing Frameworks," 2024 International Conference on Computing and Intelligent Reality Technologies (ICCIRT), Coimbatore, India, 2024, pp. 1-6, doi: 10.1109/ICCIRT59484.2024.10922035.
19. Anusha, P. (2025). Developing Explainable and Ethical AI Chatbots for Healthcare Decision Support Systems. Advances Journal of Artificial Intelligence and Autonomous Intelligence in Artificial Intelligence and Machine Learning; Review, 2(3), 22.