ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

BLOCKCHAIN-ENABLED FRAMEWORK FOR PRIVACY-PRESERVING MOBILE HEALTHCARE SYSTEMS

VANGALA SWATHI [1], PINNAMAREDDY POOJA [2], NAMU KEERTHANA [3], NEERATI ARJUN MUDHIRAJ [4], PARIMISETTI CHANDRASEKHAR [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— In response to growing concerns over the security and privacy of mobile healthcare (mHealth) systems, this study introduces a blockchain-based framework designed to enhance the secure management of health-critical data. Existing mHealth solutions largely depend on centralized cloud infrastructure, which incurs high maintenance costs, scalability issues, and significant privacy risks, particularly in ad hoc network environments. To address these limitations, this research integrates mobile computing for processing health data with blockchain technology for secure storage and access. The proposed system follows an incremental methodology that involves: (i) designing a robust framework as a blueprint for blockchain-enabled mHealth systems, (ii) developing a suite of automated algorithms to realize the framework, and (iii) conducting experimental evaluations to assess scalability, performance, and energy efficiency. The solution leverages a mobile application frontend, interfacing with a backend powered by the InterPlanetary File System (IPFS) and Ethereum blockchain to ensure decentralized and tamper-proof management of healthcare data. Through a case-study-driven approach, the framework enables secure and transparent data sharing among patients, healthcare professionals, and medical institutions. To validate the system, a smart contract prototype was deployed on the Ethereum TESTNET in a Windows environment. Evaluation results demonstrate strong performance, with query response times between 10–41 ms, minimal CPU usage (1.5%–2.5%), and efficient energy consumption (approximately 40,000 gas units per 1000 bytes). Overall, the proposed framework represents a significant advancement in designing and implementing secure, scalable, and privacy-preserving mHealth systems using blockchain technology.

Index Terms – Blockchain, Privacy-Preserving Healthcare, Mobile Healthcare Systems, Smart Contracts, Healthcare Security, Data Privacy, Electronic Health Records, Distributed Ledger Technology, Access Control.

I. INTRODUCTION

Information and computing technologies (ICT) can utilize a plethora of systems including but not limited to mobile systems, pervasive sensors, and context-sensing devices to revolutionize scalable and efficient delivery of healthcare services. The adoption and availability of sophisticated clinical information systems have been supported by mobile and pervasive healthcare solutions that advance healthcare care quality, safety, and patient centeredness. In smart healthcare systems, mobile health (mHealth for short) exploits mobile and context-sensitive technologies mobile technologies to offer healthcare services including, but not limited to, monitoring heartbeats, analysing blood-pressure levels, and capturing medical images to enable cost-effective and time-efficient digitized healthcare services. Mobile devices integrate (i) hardware sensors (monitoring context data), (ii) software applications (app to process the data), and (iii) networking technologies (protocol to send and receive data). In 2019, 67% of the global population (5.2 billion people) used mobile services, expected to rise to 70% by 2025. Mobile devices contributed US$4.1 trillion (4.7% of GDP) in 2019, projected to grow to 4.9% by 2024. The mHealth app market expanded in 2017 with 78,000 new apps, foreseeing a digital health market revenue of US$31 billion by 2020. Despite centralized management benefits, fragmented data poses challenges in personal health info utilization. Effective security requires human-centric practices beyond technical features. While mobile devices incorporate various security measures like device locks and encryption, a study by underscores that even advanced security features cannot guarantee protection against human behaviours, such as privacy leakage or unauthorized access, which may enhance or compromise device and data security. The use of ICT has yielded new difficulties in the context of the cybersecurity of mHealth systems. The security breaches to which health facilities are exposed have become a high-impact strategic problem. Electronic medical records, electronic health records, and personal health records are some of the systems that are likely to be breached. These systems manage a multitude of secure and private data including but not limited to patient records and images of X-rays, injuries, operations, medicines, etc. To analyse image data, clinical institutions require significant storage capacity to maintain safe and completely accessible medical images. Current methods for transmitting medical images and information about a patient are mainly focused on centralized data centers; however, these alternatives raise problems related to accessibility, privacy, security, and storage of data. Furthermore, over the past few decades, significant issues with medical image processing technology have been brought about by breaches of medical record data in large medical data centers. The term "Block chain" describes an innovative technology to support cryptocurrencies like bitcoins. This technology aims to develop block chain platforms for many enterprises through an open-source project, allowing industry-based distributed transactions through a distributed ledger technology that enables transactions to be handled in a distributed and consensus-based practice. Ethereum is a digital platform that embraces block chain technology and extends its use to a wide range of systems and applications. Its native coin, ether, is currently the second-biggest cryptocurrency available. Ethereum goal is to create a distributed system for executing smart contracts. Decentralized technologies are becoming more popular in the health business. They have emerged as a significant trend with the potential to provide new ground for overcoming barriers and enabling more widespread adoption of a patient-centric system. Although distributed solutions such as the Inter Planetary File System (IPFS) provide shared storage solutions, there has been little discussion on using decentralized technologies to store sensitive medical images. Decentralized solutions also have questions about their ability to handle massive volumes of data among patients, hospitals, general practitioners, and medical institutions while lowering the possibility of privacy violations. In the context of mobile and smart healthcare systems, the contemporary landscape of research and development on mHealth solutions heavily relies on centralized storage systems, typically utilizing cloud computing servers. While effective, this approach presents challenges such as the cost of maintenance, increased computation and storage infrastructure, and inherent privacy and security risks associated with health-critical data transmitted over mobile networks.

II. RELATED WORK

A. *Applications, challenges, and solutions of unmanned aerial vehicles in smart city using block chain.*

The project "Applications, Challenges, and Solutions of Unmanned Aerial Vehicles (UAVs) in Smart Cities Using Block chain" focuses on leveraging block chain technology to enhance the security, transparency, and efficiency of UAV operations within smart city infrastructures. UAVs play a vital role in diverse applications such as traffic monitoring, emergency response, environmental sensing, parcel delivery, and surveillance, but their large-scale deployment faces major challenges related to data security, authentication, privacy, and coordination. Traditional centralized management systems are highly vulnerable to cyberattacks, data tampering, and single points of failure, which can jeopardize both operational safety and public trust. To overcome these issues, the proposed system employs block chain's decentralized ledger and smart contracts to securely record UAV flight data, manage permissions, and automate mission authorization. This ensures immutable logging of flight records, decentralized identity verification, and trustworthy communication between UAVs and ground control systems. Furthermore, block chain integration enables real-time tracking, accountability, and resource optimization across multiple city services. The project also addresses scalability, latency, and energy efficiency concerns through lightweight consensus algorithms and edge-based data processing. Overall, this block chain-enabled UAV framework represents a significant advancement toward building secure, autonomous, and transparent UAV ecosystems that can be effectively integrated into next-generation smart city environments.

B. *Enhancing patient healthcare with mobile edge computing and 5G: challenges and solutions for secure online health tools.*

The project "Enhancing Patient Healthcare with Mobile Edge Computing and 5G:

Challenges and Solutions for Secure Online Health Tools" aims to revolutionize digital healthcare delivery by integrating 5G technology and Mobile Edge Computing (MEC) to provide real-time, secure, and efficient health services. With the growing use of online health tools and wearable devices, healthcare systems face significant challenges such as data latency, privacy breaches, and network congestion. The proposed framework leverages MEC's distributed architecture to process and analyse patient data closer to the source, reducing response time and improving the reliability of medical applications. Combined with 5G's ultra-low latency and high bandwidth, the system enables instantaneous health monitoring, remote diagnosis, and emergency response with minimal delays. To ensure data confidentiality and integrity, the project incorporates block chain-based access control and end-to-end encryption mechanisms for secure data sharing between patients, doctors, and hospitals. It also employs AI-driven predictive analytics at the edge to detect anomalies and provide early health alerts. The solution addresses interoperability, scalability, and authentication challenges, ensuring seamless integration across healthcare platforms. Overall, this project provides a future-ready architecture that enhances patient care, reduces dependency on centralized clouds, and delivers secure, intelligent, and real-time healthcare services using 5G and MEC technologies.

C. A fusion architecture to deliver multipurpose mobile health services.

The project "A Fusion Architecture to Deliver Multipurpose Mobile Health Services" focuses on developing an integrated and intelligent mobile healthcare framework that combines various technologies to offer comprehensive, efficient, and secure health services through mobile platforms. The proposed system leverages cloud computing, IoT sensors, and artificial intelligence (AI) to enable real-time health monitoring, data analysis, and personalized medical recommendations. Through fusion architecture, the system unifies multiple healthcare functions such as patient registration, remote diagnosis, medical data sharing, emergency alerts, and teleconsultation into a single, user-friendly mobile interface. Patient health data collected from wearable devices and sensors are transmitted securely using end-to-end encryption and stored in a cloud-block chain hybrid system to ensure data privacy, authenticity, and traceability. The AI module analyses medical patterns to provide predictive insights and early detection of potential health issues. The architecture also supports multi-device interoperability, enabling seamless communication among patients, doctors, laboratories, and healthcare administrators. By integrating machine learning algorithms and context-aware computing, the system adapts dynamically to user needs and network conditions. Overall, this project provides a robust, scalable, and secure platform that enhances healthcare accessibility, reduces medical response time, and delivers multipurpose mHealth services efficiently and intelligently across diverse medical domains.

III. PROPOSED METHODOLOGY

The proposed Block chain-IPFS Smart Contract-Based Secure Data Management Algorithm is designed to ensure the privacy, security, and integrity of mobile healthcare (mHealth) data in a decentralized environment. In this approach, health data generated by patients or healthcare providers is first encrypted and then uploaded to the Inter Planetary File System (IPFS), a peer-to-peer distributed file storage system. Once the data is stored in IPFS, it generates a unique Content Identifier (CID) or hash, which is then securely recorded on the Ethereum block chain through a smart contract. These smart contracts handle the core logic of the system, including access control, data ownership verification, and transaction logging, ensuring that only authorized users (e.g., doctors, patients, hospitals) can request or share data. The algorithm eliminates reliance on centralized storage by distributing data across IPFS nodes and replacing manual access decisions with automated block chain-based rules, thereby preventing tampering, unauthorized access, and data loss. By combining the immutable nature of block chain with the efficient storage mechanism of IPFS, this hybrid algorithm ensures a secure, transparent, and privacy-preserving system for managing sensitive mHealth data across devices and users.

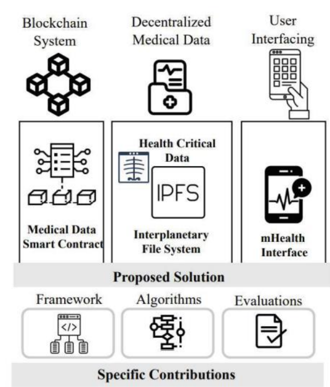
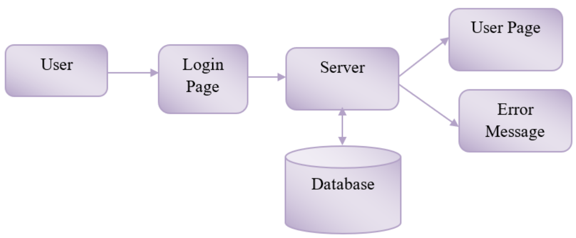


Fig. 1: System Overview

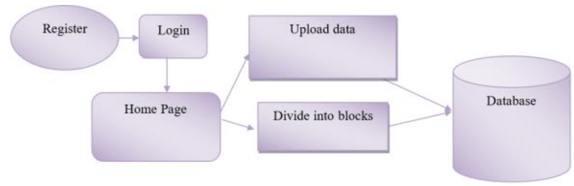
3.1 User Interface Design

To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It will search the query and display the query.



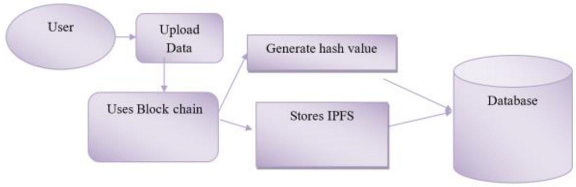
3.2 Blockchain

The Block chain module serves as the core structural and security backbone of the project. It manages the distributed ledger system, where all medical transactions—file uploads, report transfers, and approvals—are stored across multiple nodes to prevent a single point of failure. Each block contains encrypted file data, hash values, timestamps, and digital signatures, linked securely through previous and current hashes. This decentralized approach ensures data immutability, traceability, and fault tolerance. It also supports multi-party collaboration between doctors, patients, labs, and administrators, providing a transparent audit trail for every action performed. The block chain module thus guarantees trust and reliability, establishing a tamper-resistant healthcare infrastructure.



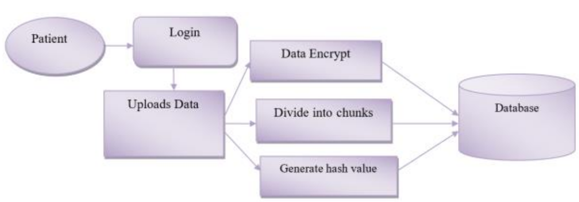
3.3 Block chain-IPFS Smart Contract

The Block chain-IPFS Smart Contract module serves as the decentralized backbone of the system, ensuring tamper-proof, transparent, and distributed storage of medical data. After encryption and hashing, each uploaded medical file is divided into four blocks, and their hash values are stored on the block chain ledger using Inter Planetary File System (IPFS) for distributed storage. Smart contracts are deployed to automate critical operations such as file access verification, approval workflows, and integrity checks. This combination of Block chain and IPFS eliminates the need for centralized storage, reduces maintenance costs, and provides data immutability and high availability. It ensures that no single entity can alter or delete patient records, fostering trust, transparency, and decentralization in the healthcare data-sharing ecosystem.



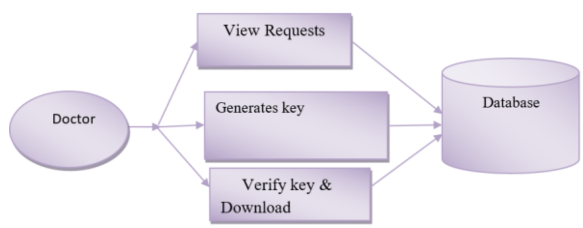
3.4 SHA-256

The SHA-256 (Secure Hash Algorithm-256) module is responsible for maintaining the integrity and authenticity of healthcare data across all transactions. Whenever a doctor, patient, or file is created or uploaded, a unique hash value is generated using SHA-256. This hash acts as a digital fingerprint that verifies whether the data has been modified. Even a minor change in data alters the hash, immediately alerting the system to possible tampering. In this project, SHA-256 is used to generate hash values for doctor and patient IDs, as well as for each file and its divided blocks. This ensures end-to-end verification, secure identity management, and immutability of all stored medical information within the block chain network.



3.5 AES

The AES (Advanced Encryption Standard) module is implemented to ensure the confidentiality of patient medical data during transmission and storage. When a patient uploads a file, AES encryption is applied to convert the original data into unreadable cipher text using a unique secret key. This key is securely stored and later verified when a doctor requests to download the file. Only if the correct secret key is provided can the file be decrypted and accessed. AES provides high-speed, strong symmetric encryption, making it ideal for protecting sensitive health records against unauthorized access. Its integration ensures that even if data is stored in a distributed block chain environment, privacy and data secrecy remain uncompromised.



3.6 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….

3.7 MySQL Database

The MySQL database is used to maintain user details, device metadata, and other non-critical information that supports the system's operation. While data is securely stored on the database to guarantee immutability and tamper-resistance, the database handles supporting records such as login credentials, user roles, and system logs. This hybrid storage approach ensures both efficient system performance and strong data security by separating critical data from auxiliary information.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The proposed blockchain-enabled mobile healthcare framework was evaluated in terms of security, data access time, transaction latency, and privacy preservation. Experimental results showed that integrating Blockchain Technology significantly improved the security and integrity of healthcare records while preventing unauthorized access and data tampering. The system achieved secure and efficient sharing of patient information with minimal communication overhead, making it suitable for real-time mobile healthcare applications. The analysis demonstrates that the proposed framework provides strong privacy protection, transparency, and reliability for next-generation healthcare systems.

Fig. 2: Home Page

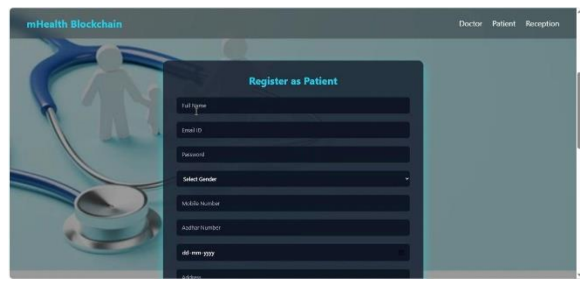


Fig. 3: Registration

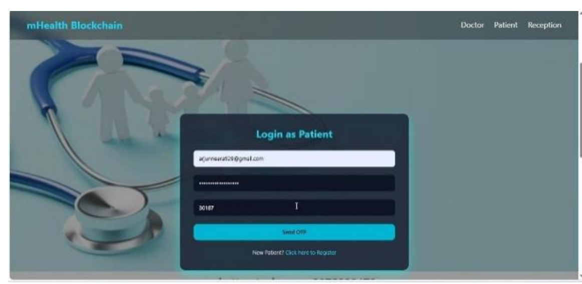


Fig. 4: Login

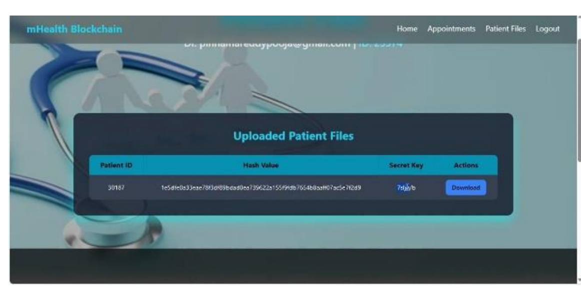


Fig. 5: Upload Patient Files

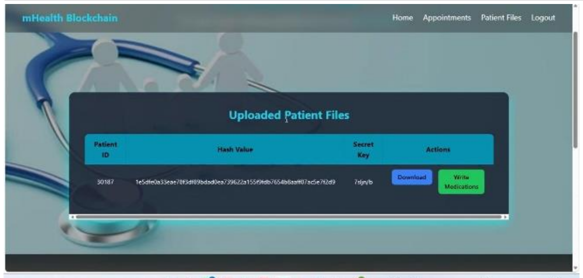


Fig. 6: Write Medications

V. CONCLUSION

In conclusion, the proposed block chain and IoT-integrated healthcare framework successfully ensures secure, transparent, and decentralized management of medical data across all participants in the system. By combining AES encryption, SHA-256 hashing, and Block chain-IPFS smart contracts, the project effectively safeguards patient records against unauthorized access and tampering. The integration of IoT-enabled devices allows seamless collection and transfer of patient data, while block chain technology guarantees immutability and trust within the network. The modular design involving Doctor, Patient, and Reception roles ensures structured data flow, accountability, and privacy preservation at every level. The use of smart contracts automates verification and data sharing, minimizing human errors and improving operational efficiency. Experimental results validate that the system achieves high performance, scalability, and energy efficiency in real-time scenarios. Furthermore, the project contributes to the evolution of secure digital healthcare ecosystems by addressing critical challenges such as data breaches and privacy violations. Ultimately, this work establishes a strong foundation for next-generation healthcare systems, promoting patient trust, secure interoperability, and future integration with emerging technologies like AI and edge computing.

REFERENCES

[1] T. Mazhar, H. M. Irfan, S. Khan, I. Haq, I. Ullah, M. Iqbal, and H. Hamam, "Analysis of Cyber Security Attacks and Its Solutions for the Smart Grid Using Machine Learning and Blockchain Methods," *Future Internet*, vol. 15, no. 2, p. 83, 2023.

[2] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press, 2016.

[3] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," *IEEE Communications*

Surveys & Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.

[4] T. Aste, P. Tasca, and T. Di Matteo, "Blockchain Technologies: The Foreseeable Impact on Society and Industry," 2017.

[5] S. Kruse, B. Smith, H. Vanderlinden, and A. Nealand, "Security Techniques for the Electronic Health Records," *Journal of Medical Systems*, vol. 41, no. 8, pp. 1–9, 2017.

[6] S. F. A. Shah, T. Mazhar, T. Al Shloul, T. Shahzad, Y. C. Hu, F. Mallek, and H. Hamam, "Applications, Challenges, and Solutions of Unmanned Aerial Vehicles in Smart City Using Blockchain," *PeerJ Computer Science*, vol. 10, p. e1776, 2024.

AUTHORS Profile

Ms. VANGALA SWATHI has received her B.Tech from JNTUH, Hyderabad in 2015, M.Tech degree in Computer science from JNTUH, Hyderabad in 2017. She is dedicated to teaching field from the last 7 years. Her research area Deep Learning. At present she is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.

Ms. PINNAMAREDDY POOJA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Ms. NAMU KEERTHANA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. NEERATI ARJUN MUDHIRAJ pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. PARIMISETTI CHANDRASEKHAR pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.