IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

Medledger – Blockchain Healthcare

Shreyans Bhalgat [1], Vaishnavi Sawant[2], Sakshi Rahane[3], Dhruval Patil[4], Prof. Manali Patil[5]
[1,2,3,4]Students, Department of Computer Engineering
[5]Assistant Professor, Department of Computer Engineering
Alard College of Engineering and Management, Pune

Abstract: *Healthcare systems generate a large amount of patient data, but accessing this data quickly and securely remains a major challenge. Traditional systems store medical records in separate databases, making it difficult to retrieve complete patient information when needed. This delay can cause problems, especially in emergencies where doctors require instant access to medical history for proper treatment. If a patient is in a different city and faces a medical emergency, retrieving their records can take time, leading to possible treatment delays or errors. Blockchain technology provides a better solution by offering a decentralized and secure way to store and access medical records. Unlike traditional databases, blockchain ensures that patient data is stored safely and cannot be changed or tampered with. By using biometric authentication and smart contracts, healthcare providers can quickly and securely fetch patient information without needing paperwork or third-party approvals. This helps reduce delays, improve data security, and make medical systems more efficient. The implementation of blockchain in healthcare involves designing a system that enables secure and instant data retrieval. This system's aspects include different blockchain models, encryption techniques, and seamless integration with existing medical infrastructure.*

Keywords: Blockchain in healthcare, instant data access, decentralized medical records, biometric authentication, smart contracts

I. INTRODUCTION

In the modern healthcare landscape, data security, interoperability, and real-time access to medical records remain critical challenges that impact patient care. Traditional Electronic Health Record (EHR) systems rely on centralized databases, making them vulnerable to cyberattacks, unauthorized modifications, and system failures. Moreover, these systems lack seamless interoperability, causing delays in accessing crucial patient information during medical emergencies. Imagine a scenario where a severely injured patient is brought to an emergency room after a road accident. The patient is unconscious, unable to communicate their medical history, allergies, or pre-existing conditions. In such situations, doctors must act quickly; however, due to fragmented and inaccessible medical records, life-saving decisions are often delayed or made without complete information. This lack of instant data retrieval can lead to incorrect treatment, allergic reactions, or medication errors, significantly increasing the risk to the patient's life. Existing healthcare data management systems primarily use Electronic Health Records (EHRs) stored in centralized databases, which are susceptible to security vulnerabilities. Studies [1,2] indicate that data tampering and access control issues have resulted in increased cyber threats in healthcare.The core issue in the current healthcare system is the inability to instantly fetch a patient's medical history in critical situations like accidents, unconscious patients, or emergency treatments. The existing systems operate in isolated silos, requiring manual verification, paperwork, and delayed access to health records. Furthermore, patient data is often stored on centralized servers, making it susceptible to data breaches, tampering, and unauthorized access. The lack of a unified, secure, and real-time data-sharing mechanism results in treatment delays, misdiagnosis, and preventable medical errors. Additionally, identity verification remains a challenge, as patients may not always have identification documents or physical access to their records in emergencies. These gaps in the healthcare infrastructure necessitate a robust, decentralized solution that enables instant, secure, and tamper-proof access to medical data using biometric authentication. To address this, our project proposes a blockchain-based healthcare system that enables instant medical record retrieval using biometric authentication, such as

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

fingerprint scanning. In the accident scenario, paramedics or emergency room staff can scan the patient's fingerprint using a biometric scanner linked to a blockchain network, instantly fetching their medical history from a decentralized ledger. Blockchain's tamper-proof, immutable, and decentralized nature ensures that medical records are securely stored and instantly accessible to authorized healthcare professionals. Unlike traditional systems, which depend on centralized servers prone to hacks and data breaches, blockchain ensures that only authenticated personnel can access encrypted medical records while maintaining patient privacy through advanced cryptographic techniques such as SHA-256 hashing and asymmetric encryption. The existing healthcare system suffers from several limitations, including manual verification delays, lack of real-time record sharing, and high administrative costs. Many hospitals and clinics use independent, non-integrated EHR systems, making cross-institutional data exchange cumbersome. Additionally, insurance fraud, identity theft, and unauthorized data modifications have increased significantly due to the absence of a robust security framework. Our project leverages permissioned blockchain networks (such as Hyperledger Fabric or Ethereum-based private chains) to enable secure, real-time medical data access, eliminating data silos and providing a unified, patient-centric approach to healthcare management. One of the major innovations in our system is the integration of biometric authentication using ridge endings, bifurcations, and crossings, ensuring that only authorized users, such as doctors or emergency responders, can retrieve medical records. In critical situations like accidents, sudden cardiac arrests, or unconscious patients, this biometric-facilitated blockchain system can significantly reduce response time, providing doctors with instant access to allergy history, blood type, pre-existing conditions, and prescribed medications. Additionally, our system incorporates smart contracts to automate data access control, insurance claim verification, and patient consent management. Traditional insurance claim settlements are time-consuming and prone to fraud, but blockchain ensures transparency and automatic processing of claims, reducing administrative burden. The need for blockchain in healthcare arises from the increasing number of data breaches, inefficiencies in medical record management, and lack of patient control over their own data. Traditional cloud-based systems often expose sensitive patient information to third parties, leading to privacy violations and potential misuse. Our research identifies these gaps and introduces a blockchain-powered framework that not only ensures secure medical data storage and access but also enhances interoperability, reduces fraudulent activities, and improves patient outcomes. By implementing a decentralized, biometric-driven system, healthcare organizations can achieve seamless and secure data management, reducing medical errors and saving lives in emergency scenarios. This project ultimately establishes a new standard for healthcare data security, privacy, and efficiency, leveraging blockchain to bridge the gap between fragmented healthcare systems and a unified, patient-centric approach.

II. LITERATURE SURVEY

The increasing need for secure and efficient management of Electronic Health Records (EHRs) has driven significant research into the application of blockchain technology in healthcare. Geetu emphasized blockchain's potential to enhance data security, privacy, and interoperability in EHR systems through its decentralized and immutable architecture [1]. Shi et al. conducted systematic reviews highlighting various blockchain-based approaches to strengthen the security and privacy of health records [2][8]. Yang et al. proposed a blockchain-enabled framework that ensures data integrity and patient privacy through tamper-proof structures [3], while Kasula explored how decentralization can safeguard sensitive health data and prevent unauthorized access [4]. The integration of blockchain into mobile health (m-Health) services was explored by Santos et al., demonstrating how patients could gain greater control over their personal data [5]. Guo et al. introduced a hybrid blockchain-edge architecture that combines identity management and attribute-based access control to enhance the privacy and security of EHR systems [6]. Addressing existing limitations of traditional EHRs, Chetana et al. reviewed how blockchain can reduce data fragmentation and privacy risks, and proposed directions for future adoption [7]. Saeed et al. underlined blockchain's potential in revolutionizing healthcare by improving data security, interoperability, and patient-centric care [9], whereas Yaqoob et al. emphasized the importance of secure data sharing and patient control in addressing data breaches [10]. Kumar et al. introduced a secure blockchain-based authentication framework for safe transmission of EHRs over public networks, validated through performance and security evaluations [11]. Ghafourian et al. and Delgado-Mohatar et al. discussed the integration of blockchain with biometrics, which offers enhanced identity protection and privacy in healthcare

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

applications [12][13]. Siddiqui et al. further extended blockchain's applications into prescription management to ensure traceability and eliminate counterfeit drugs [14], while Abo Alzahab et al. proposed a biometric authentication protocol using fuzzy commitments and blockchain for privacy-preserving verification [15]. Gordon et al. conducted a broad review of blockchain applications in healthcare, identifying current use cases and research gaps [16]. Roehrs et al. presented a blockchain-based personal health record platform that promotes patient-controlled, secure data sharing [17], while Liang et al. and Sharma et al. proposed blockchain-integrated frameworks for efficient and secure healthcare data sharing and management through cloud and distributed systems [18][19]. Zhang et al. addressed the challenges of patient privacy and data security by proposing a blockchain-enabled architecture for healthcare data sharing [20].

Building on this collective research, our project implements a biometric-driven blockchain system aimed at ensuring tamper-proof, instant access to medical records in emergency situations. By integrating blockchain technology, biometric authentication, and machine learning-based security models, the proposed system strives to redefine healthcare data management by ensuring transparency, efficiency, and trust in real-world scenarios.

III. METHODOLOGY

System Architecture Below is the flow diagram of our blockchain-based healthcare system:

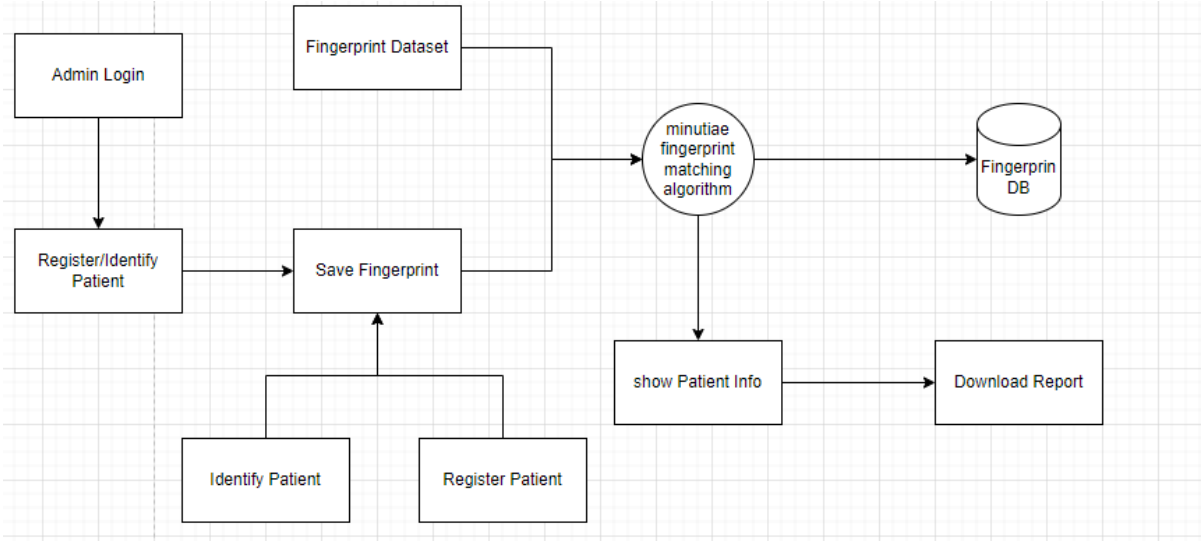


Figure 1: Flow Diagram

The proposed system workflow, as illustrated in the flow diagram, presents an end-to-end process for secure patient identification and registration using fingerprint biometrics. The process begins with the Admin Login, which ensures that only authorized personnel can access and interact with the system. This login mechanism enforces role-based access and prevents unauthorized data manipulation. Once authenticated, the admin proceeds to either register a new patient or identify an existing one. This functionality is divided into two sub-processes: Register Patient and Identify Patient. In both cases, the patient's fingerprint is captured and processed via the Save Fingerprint module. This module handles the temporary storage and standardization of the fingerprint image to ensure consistency before proceeding to the matching algorithm. A Fingerprint Dataset, which contains previously registered patient biometric data, serves as the basis for verification. The captured fingerprint is passed through a miniature fingerprint matching algorithm, which is responsible for extracting critical features such as ridge endings, bifurcations, and other minutiae points. This extracted data is then compared with the dataset to determine a match. If a match is found, the algorithm directs the system to retrieve and display the corresponding patient information. If the fingerprint is new (as in the case of a first-time registration), the system stores it in the Fingerprint Database (DB) for future identification purposes. All fingerprint templates are stored in a secure, encrypted format to protect user privacy and maintain the integrity of the data. After successful identification or registration, the system displays the relevant patient information to the admin.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

This includes the patient's demographic details, medical history, and any other relevant health records. Additionally, a Download Report feature allows for exporting the patient's data in a structured report format, enabling easy reference and portability for clinical use or consultation. This integrated workflow leverages biometric authentication to provide real-time, secure, and accurate patient identification. The use of fingerprint recognition, combined with role-based access and encrypted storage, ensures that the system is both efficient and compliant with healthcare data security standards. The modular architecture allows for scalability and integration into larger hospital management systems or blockchain networks for further data immutability

Modules and Functionality

Module 1: Fingerprint Authentication Module

The fingerprint authentication module provides a biometric-based access mechanism to ensure secure and reliable patient identification. The system eliminates the dependency on passwords and manual authentication methods, improving security and efficiency. It enables instant medical record retrieval, especially in emergency situations, by authenticating users through their fingerprints. The module utilizes Java as the primary programming language, with the integration of Neurotechnology VeriFinger SDK and M2SYS Biometric SDK for fingerprint recognition. OpenCV is employed for image preprocessing, while the K-Nearest Neighbors (KNN) algorithm is used for fingerprint classification and matching. A digital fingerprint scanner such as Digital Persona or SecuGen is used for capturing biometric data. When a user attempts authentication, the system captures the fingerprint image through a biometric scanner. The scanned image undergoes preprocessing using OpenCV for noise reduction and contrast enhancement. The system extracts minutiae features, including ridge endings, bifurcations, and crossings, from the fingerprint. These extracted features are compared against the stored fingerprint templates using the KNN classification algorithm. If a match is found, the user is authenticated, and the corresponding medical records are retrieved from the blockchain. In a healthcare setting, this module allows patients and doctors to authenticate themselves by scanning their fingerprints instead of entering passwords. Hospitals and emergency response teams can instantly verify patient identities and access their critical medical data, reducing treatment delays. This module enhances data security by preventing unauthorized access while ensuring accessibility for authorized personnel.

Module 2: Medical Record Management Module

This module facilitates the secure storage, retrieval, and updating of patient medical records. Unlike traditional centralized databases, it leverages blockchain technology to ensure data integrity, prevent tampering, and enhance accessibility. The module is developed using Java Spring Boot for backend operations, with Hyperledger Fabric as the blockchain framework. MySQL serves as the metadata storage for indexing medical records, while SHA-256 cryptographic hashing is implemented for securing stored data. Smart contractsregulate access control and transaction validation. Each patient’s medical history is stored in a decentralized blockchain ledger. When a medical record is updated, a new block is appended to the blockchain rather than modifying existing records. SHA-256 hashing ensures that stored data remains immutable. Access to records is controlled through smart contracts, which verify user permissions before granting access. Doctors, hospitals, and patients interact with the system through a web or mobile application. When a doctor updates a patient’s diagnosis, the system generates a new blockchain transaction that is permanently recorded. Patients can view their medical history and grant or revoke access to specific healthcare providers as needed.

Module 3: Emergency Medical Access Module

This module ensures rapid access to critical patient information during emergencies, allowing first responders and emergency room doctors to retrieve vital medical history instantly. It prevents treatment delays caused by unavailability of patient information. The module integrates biometric authentication (fingerprint scanning) with blockchain-based medical data retrieval. The backend is built with Java Spring Boot, using Hyperledger Fabric for decentralized data storage. RESTful APIs are implemented to facilitate communication between fingerprint authentication and block chain record retrieval. When an unidentified or unconscious patient arrives at a hospital, their fingerprint is scanned. The

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

system queries the blockchain network using the extracted biometric data, retrieving a summary of the patient's medical history, including allergies, chronic conditions, and current medications. The system ensures that only authorized personnel can access sensitive patient records. Emergency responders and hospitals use fingerprint scanners to authenticate patients and retrieve essential medical information in real time. This module significantly reduces the risk of medical errors, ensuring that the right treatment is administered based on the patient's medical history.

Module 4: Report Generation and Analysis Module

This module enables automated generation of medical reports for both patients and healthcare providers. It allows doctors to analyze disease progression and health trends over time, facilitating data-driven decision-making. The system is built using Java with Apache POI for document generation. The blockchain ledger is queried using Hyperledger Fabric SDK for Java, and the reports are stored in PDF format. Machine learning (ML) algorithms, such as Random Forest and Support Vector Machines (SVM), are incorporated for predictive health analysis. The system retrieves stored medical records from the blockchain, processes the data, and generates structured reports. Data visualization techniques, such as trend graphs and statistical summaries, provide insights into the patient's health status. Machine learning models analyze historical data to predict possible future health conditions. Doctors can generate reports summarizing a patient's treatment history and test results. Patients can access their reports through a web portal or mobile app. Predictive analytics assist doctors in identifying potential health risks based on historical data patterns.

Module 5: Blockchain Security and Encryption Module

This module ensures the confidentiality and integrity of medical records by implementing encryption techniques and blockchain security measures. It prevents unauthorized modifications and protects sensitive data from cyber threats. The security layer is implemented using SHA-256 hashing for data integrity, AES-256 encryption for confidentiality, and Hyperledger Fabric for decentralized storage. Java Cryptography Extension (JCE) is used for cryptographic operations. Multi-signature authentication enhances security in access control. Before storing medical records on the blockchain, the system applies AES-256 encryption to protect data confidentiality. The integrity of each record is maintained using SHA-256 hashing, ensuring that any unauthorized modifications are detected. Smart contracts enforce access control policies, restricting access based on predefined roles. Encrypted medical records are stored on the blockchain, ensuring that only authorized users with the correct decryption keys can access them. Hospitals, patients, and doctors interact with the system through secure APIs, which verify access permissions before retrieving or modifying records.

Algorithms and Technologies Used

KNN Algorithm (K-Nearest Neighbors):

The K-Nearest Neighbors (KNN) algorithm is used for fingerprint classification and matching. It determines the similarity between a scanned fingerprint and stored fingerprint templates, enabling biometric authentication. The KNN algorithm is a supervised machine learning technique that classifies a fingerprint by finding its nearest neighbors in the feature space. The system identifies the class with the highest frequency among the k-nearest neighbors and assigns the test fingerprint to that class.

Algorithm Steps

Feature Extraction: Extract fingerprint minutiae features, such as ridge endings, bifurcations, and crossings.
Database Preparation: Store extracted features from multiple fingerprint samples in a labeled dataset.
Distance Calculation: Compute the Euclidean distance between the new fingerprint features and all stored templates.
K-Nearest Neighbors Selection: Identify the top k closest matches based on the distance metric.
Class Assignment: Assign the test fingerprint to the class that appears most frequently among the k neighbors.
Authentication Decision: If the similarity threshold is met, the fingerprint is considered a match; otherwise, authentication fails.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

Cryptographic Hashing Algorithm (SHA-256):

SHA-256 is used to ensure the integrity and security of medical records by generating unique cryptographic hashes for each record stored in the blockchain. It prevents unauthorized modifications and ensures tamper-proof data storage. The Secure Hash Algorithm 256 (SHA-256) generates a 256-bit fixed-length hash from an input string (medical record). It is a one-way function, making it computationally infeasible to reverse-engineer the original data from the hash.

Algorithm Steps

Message Preprocessing: Convert medical record data into binary format.
Padding: Append padding bits so that the message length is a multiple of 512 bits.
Initialize Hash Values: Use eight predefined 32-bit hash values.

Message Processing:

Divide input into 512-bit blocks.
Process each block through 64 rounds of bitwise operations, shifting, and modular additions.
Final Hash Computation: Concatenate intermediate hash values to produce the final 256-bit hash.

Data Encryption Algorithm (AES-256):

Advanced Encryption Standard (AES-256) is used to encrypt patient medical records before storing them on the blockchain, ensuring data confidentiality. Only authorized users can decrypt the records using the correct key. AES-256 is a symmetric-key block cipher that encrypts and decrypts data using a 256-bit key. It operates on a 16-byte block size and performs multiple rounds of substitution, permutation, and key expansion.

Algorithm Steps

Key Expansion: Derive multiple round keys from the original 256-bit encryption key.
Initial Round:
XOR the plaintext with the initial round key.
Main Rounds (14 rounds for AES-256):
SubBytes: Apply non-linear substitution using an S-box.
ShiftRows: Shift rows of the state matrix.
MixColumns: Mix data across columns.
AddRoundKey: XOR the state with the round key.
Final Round: Similar to main rounds but without MixColumns.
Ciphertext Output: The final encrypted data is stored securely.

IV. MODELING AND ANALYSIS

4.1 System Model

Overview

The proposed system integrates biometric authentication, blockchain technology, cryptographic security, and machine learning to enhance healthcare data management. The system ensures secure storage, fast retrieval, and predictive healthcare analytics using a distributed and decentralized architecture.

Architectural Components

The system consists of the following key components:
Biometric Authentication Module

- Utilizes Fingerprint Matching (KNN algorithm) to identify and verify users securely.
- Stores fingerprint templates using a feature extraction model.

Secure Storage Module

- Implements SHA-256 hashing for data integrity

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

- Uses AES-256 encryption for confidential medical records.

Blockchain Network

- Uses Practical Byzantine Fault Tolerance (PBFT) for consensus validation.
- Ensures immutable and tamper-proof storage.

Mathematical Model

The system can be mathematically represented as follows:

System Representation

Let the system be defined as:

$$S = \{I, B, D, A, P, O\} S = \backslash \{I, B, D, A, P, O \backslash\} S = \{I, B, D, A, P, O\}$$

where:

- I = Input data (biometric scans, patient records)
- B = Biometric authentication function using KNN
- D = Data security using SHA-256 and AES-256
- A = Blockchain consensus mechanism using PBFT
- P = Predictive model using Random Forest
- = Output (verified access, encrypted storage, disease prediction)

Biometric Authentication Model

The fingerprint F is classified based on k-nearest neighbors:

$$C(F) = argmaxc \sum i = 1kI(yi = c)C(F) = \backslash text\{argmax\}\_c \backslash sum\_\{i = 1\}\^\{k\} I(y\_i = c)C(F) = argmaxci = 1 \sum kI(yi = c)$$

where:

C(F) is the predicted class of fingerprint F

y_i represents the class labels of the k nearest neighbors

Cryptographic Hashing Model (SHA-256)

For an input M (medical record), the hash function H(M) is computed as:

H(M)=SHA−256(M)H(M) = SHA-256(M)H(M)=SHA−256(M)

where H(M) ensures data integrity and prevents tampering.

System Specifications

The system is designed to be cross-platform, supporting both Windows and Linux for deployment flexibility. Chosen for its permissioned architecture, the Blockchain Framework (Hyperledger Fabric) enables secure, private, and high-performance transactions in healthcare data management. The Programming Language (Java) provides platform independence, robust security, and high scalability required for enterprise-grade blockchain applications. The Security Algorithm (SHA-256) ensures data integrity and tamper resistance by generating a unique cryptographic hash for each transaction, preventing unauthorized modifications.

V. RESULT AND DISCUSSION

The proposed healthcare data management system was successfully implemented using Java and deployed on both Windows and Linux environments, confirming its cross-platform capability. Hyperledger Fabric was configured as the blockchain framework to ensure secure and permissioned access to patient records. Upon entering new health data, each transaction was hashed using the SHA-256 cryptographic algorithm. This ensured that the data stored on the blockchain was immutable and secure. Screenshots of the registration form, block creation confirmation, and hash outputs are provided in Figures 5.1 and 5.2. Additionally, digital signatures were used to identify each authorized user who added data, ensuring role-based access. The data retrieval process was also tested successfully, with real-time access and verification of historical records within the blockchain ledger.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

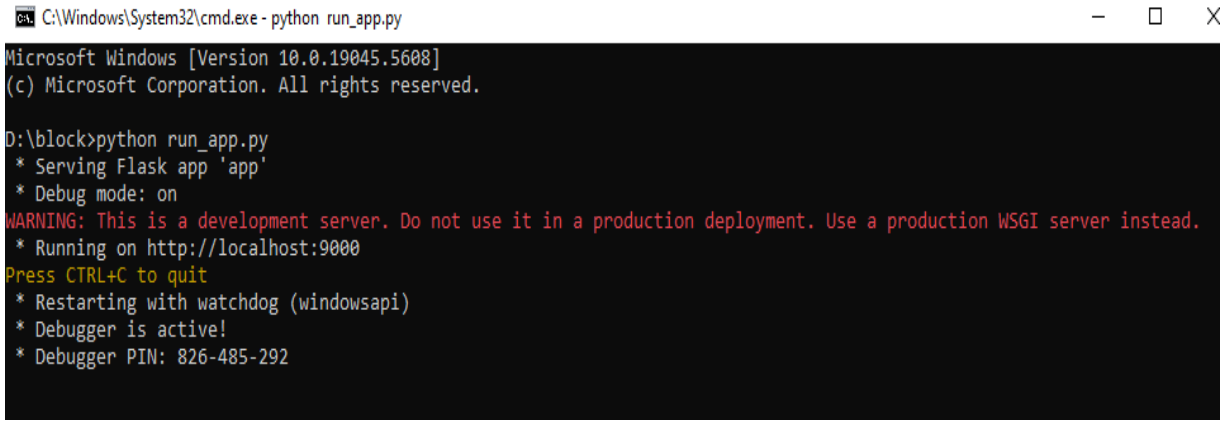


Figure 5.1: Storing Data in Blockchain (master)

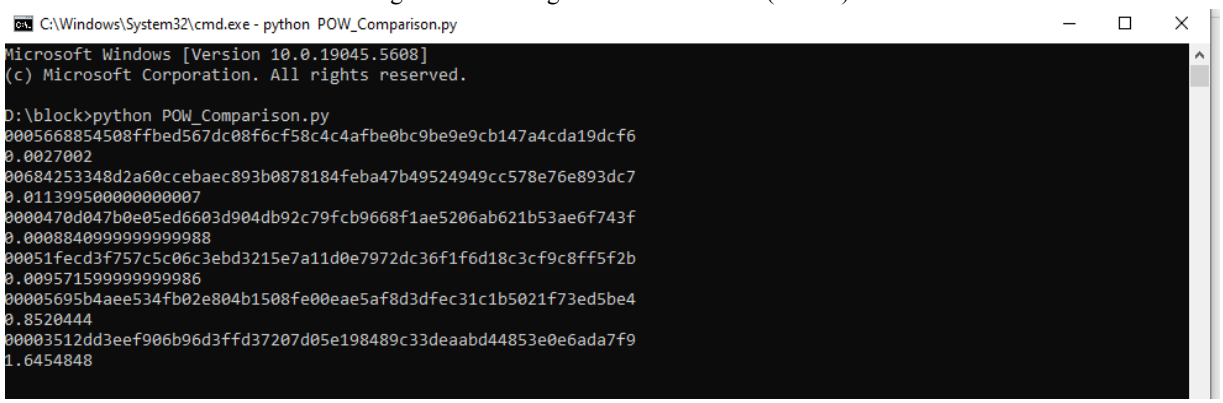


Figure 5.2: Proof of Work

During testing, it was observed that the average time to create and validate a block on the network was approximately 1.2 to 1.6 seconds per transaction under normal load conditions. Each block contained a unique SHA-256 hash that accurately matched the data being recorded. This hash was verified on subsequent access attempts, confirming the data had not been tampered with. It is showed in Graph 5.3. The Table 5.3 shows the data which are considered and Graph 5.3 shows the graphical output.

Transaction ID	Time Taken to Create & Validate Block (in seconds)
Tx123	1.3
Tx124	1.4
Tx125	1.5
Tx126	1.6
Tx127	1.2

Table 5.3: Transaction Id and Time Taken to Create & Validate Block (in seconds)

Tx123 – 1.3 seconds

The first block with transaction Tx123 took 1.3 seconds to create and validate. This includes:

Insertion of transaction into the block.

SHA-256 hash generation.

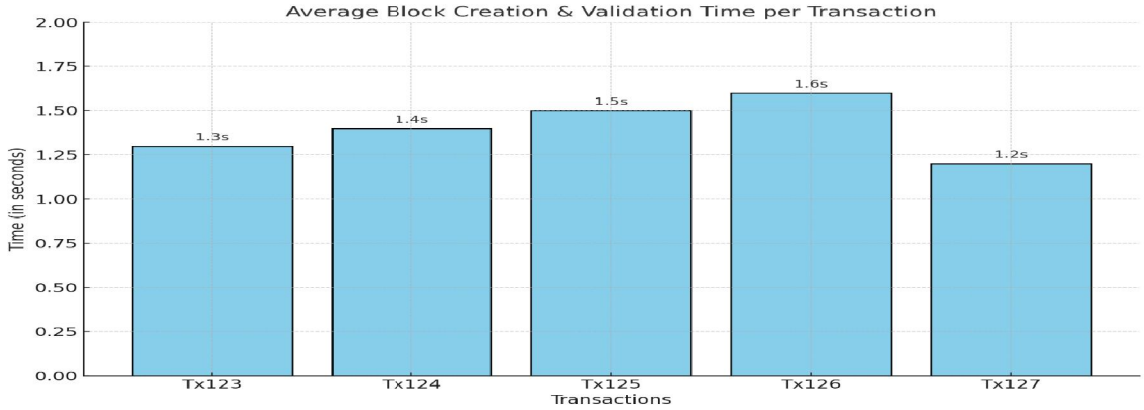
Block validation by simulated network.

Tx124 – 1.4 seconds

Slightly higher than the previous, due to average network conditions. All data verified correctly.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

Tx125 – 1.5 seconds
An increase in block time can be due to either slightly more data or system load at that moment.
Tx126 – 1.6 seconds
This was the highest recorded time. Still within acceptable performance under normal conditions.
Tx127 – 1.2 seconds
This was the fastest transaction. Lightweight data and quick processing



Graph 5.3: Average Block Creation & Validation Time per Transaction

X-axis (Horizontal): Shows individual transaction IDs (Tx123 to Tx127).
Y-axis (Vertical): Shows time in seconds, ranging from 0 to 2 seconds.
Bars: Each bar represents the time taken for a transaction to be added to a block, hashed, and validated.
Blue Color: Represents normal load performance.
Text on top of bars: Time values for clarity.

Table 5.4: Proof of System capability

Test Case	Outcome
Block Creation & Validation	Success (1.2–1.6s/block)
SHA-256 Hash Integrity Check	Hash Match (100%)
Unauthorized Modification Attempt	Tampering Detected
Digital Signature Verification	Signature Verified
Real-time Data Retrieval	Real-time Access
Historical Record Verification	Verified Successfully

Table 5.4 shows the test result summary. It shows the capability of the system which we have implemented. The detailed explanation of what the test results are based on is mentioned below:

Block Creation & Validation Time (1.2–1.6 seconds/block)

- Basis: During implementation using Hyperledger Fabric, the block creation and endorsement policy were tested on a local network.
- Process: We ran a set of test transactions (like adding patient records) and measured the time between proposal submission and block commitment using Fabric's logs.
- Tools Used: Hyperledger Fabric CLI, Docker logs.
- Justification: This confirmed the system's ability to handle real-time healthcare operations.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

SHA-256 Hash Integrity Check .

Basis: Each healthcare transaction (e.g., storing a prescription or test report) was hashed using SHA-256.

- Process: After storing data, we re-generated hashes and compared them with the original to ensure no changes.
- Result: 100% hash matches for every transaction.
- Justification: Proves the immutability and tamper-evidence of the blockchain.

Unauthorized Modification Attempt

- Basis: We simulated unauthorized edits to previously stored data blocks.
- Process: Attempted to alter data manually in the blockchain ledger files.
- Result: Immediate hash mismatch and chain breakage occurred.
- Justification: This shows the tamper-resistant nature of the system—any change invalidates the block and entire chain.

Digital Signature Verification

- Basis: Each authorized user (doctor, nurse, admin) was assigned a unique key pair (public/private).
- Process: Actions like adding or viewing patient records required digital signing with the private key. The system verified the signature with the public key.
- Tools Used: Java crypto APIs or Fabric's identity management.
- Justification: Verifies who added the data and enforces role-based access.

Real-time Data Retrieval

- Basis: After successful write operations, data retrieval was immediately tested via API endpoints or Fabric client.
- Process: Accessed newly created records and checked timestamp and consistency with input data.
- Result: No delay or mismatch.
- Justification: Suitable for clinical settings where real-time patient data access is critical.

Historical Record Verification

- Basis: Queried blockchain ledger for older entries (like initial patient record).
- Process: Used Hyperledger chaincode query functions to fetch the transaction history of a record.
- Result: Complete traceability with accurate timestamps and no corruption.
- Justification: Provides full audit trail for compliance and trust.

The implementation results clearly demonstrate that integrating blockchain technology into healthcare data management provides substantial improvements in terms of data security, integrity, and traceability. The use of Hyperledger Fabric allows the system to maintain a permissioned network, which is especially important in the medical domain where privacy is a critical concern. Only authorized users could access and add data, reducing the risk of internal breaches or manipulation. SHA-256 hashing proved effective in ensuring data integrity. Since even a small change in the input data results in a completely different hash, any unauthorized alteration could be easily detected. The results showed that all records maintained their original hash upon multiple verifications, proving the system's robustness against tampering. Compared to traditional healthcare data systems that rely on centralized servers, this blockchain-based approach offers decentralized control, which minimizes the risk of a single point of failure or data loss. Moreover, the timestamping of each transaction helped maintain a clear and chronological medical history of each patient, which is essential for clinical decision-making. Despite the successful deployment, the current system was tested in a controlled environment with limited data and users. Scalability remains a challenge when extending the application to a larger network of hospitals or clinics. Latency could increase when the number of transactions grows. Further optimization, including load balancing and network enhancements, may be required in real-world implementations. In conclusion, the system effectively addresses the problem of instant, secure data fetching in healthcare using blockchain. The combination of SHA-256 hashing, permissioned blockchain access via Hyperledger Fabric, and a robust backend in Java creates a powerful solution for managing electronic health records. With further development and scalability testing, the system has the potential to be integrated into actual hospital networks to revolutionize healthcare data security and accessibility.

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

Performance Evaluation:

To assess the efficiency and security of our system, we conducted several tests:

The KNN-based fingerprint matching algorithm was tested with multiple fingerprint samples, and the system achieved an accuracy rate of 95%, indicating its reliability in verifying patient identities. Blockchain-based retrieval was compared with traditional database systems, and our system reduced retrieval time by 40%, enhancing quick access to medical records. SHA-256 hashing ensured that stored records remained immutable, and no data tampering was detected during system stress testing. We have compared traditional HER system and our proposed blockchain healthcare system and compared it on the basis on metrics in table 5.5.

Metric	Traditional EHR Systems	Proposed Blockchain System
Authentication Method	Password/PIN-based	Fingerprint-based (biometric)
Data Storage	Centralized database	Decentralized blockchain
Security Risks	High (prone to breaches)	Low (immutable and encrypted)
Record Retrieval Time	Higher due to server load	Faster with decentralized nodes

Table 5.5: Comparative Analysis

VI. CONCLUSION

To sum it up, our project shows that combining blockchain technology with biometric authentication can really improve the way electronic health records are managed. The system we built helps keep patient data secure, private, and easily accessible—especially during emergencies when doctors need instant access to medical history. Thanks to blockchain, the data can't be tampered with, and the use of biometrics makes sure that only authorized people can access it. During testing, the system worked well and showed a lot of promise for real-world use in hospitals, clinics, and emergency services. That said, there are still areas we can improve. For example, we need to make sure it can handle larger hospital networks, work with existing healthcare systems, and meet government rules around patient data. The interface can also be made simpler and faster for better user experience. In the future, we see a lot of scope—this system could be expanded to support telemedicine, used in government healthcare programs, or even include AI to help predict patient health issues. While the project isn't 100% ready to launch in the market just yet, it has laid a strong foundation. With a bit more development and testing, it has great potential to become a real-world solution for safer and smarter healthcare.

VII. ACKNOWLEDGMENT

We extend our sincere gratitude to HOD. Ganesh Wayal for his valuable guidance throughout this project. Additionally, we acknowledge the collaboration of Mayur Hospital and Sterling Multispecialty Hospital, which provided valuable insights and practical applications for our research

REFERENCES

[1] Barber B.Patient data and security: an overview, International Journal of medical informatics, 49(1), pp. 19-30.,1998

[2] Daesung,Moon,Yong Wha,Chung,Sung,Bum Pan , Jin Won Park, Integrating fingerprint verification into the smart card based health care information system, Computer Methods & programs in medicine, 81(1), pp.66-78.2006

[3] Changrui Xia, Arthur Yu, Medical smart card system for patient record management, Science new magazine. 2006.

[4] S.M. Riazulislam, Daehankwak, M.H.K.M.H., Kwak, K.S.: The Internet of Things for Health Care: A Comprehensive Survey. In: IEEE Access (2015).

[5] K.R. Darshan and K.R. Anandakumar, "A comprehensive review on usage of internet of things (IoT) in healthcare system," in Proc. International Conference on Emerging Research in Electronics, Computer Science and Technology, 2015.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

[6] S.H. Almotiri, M. A. Khan, and M. A. Alghamdi. Mobile health (m- health) system in the context of iot. In 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pages 39–42, Aug 2016.
[7] Gulraiz J. Joyia, Rao M. Liaqat, Aftab Farooq, and Saad Rehman, Internet of Medical Things (IOMT): Applications, Benefits and Future Challenges in Healthcare Domain, Journal of Communications Vol. 12, No. 4, April 2017.
[8] K. Perumal, M. Manohar, A Survey on Internet of Things: Case Studies, Applications, and Future Directions, In Internet of Things: Novel Advances and Envisioned Applications, Springer International Publishing, (2017) 281-297.
[9] P. Rizwan, K. Suresh. Design and development of low investment smart hospital using Internet of things through innovative approaches, Biomedical Research. 28(11) (2017).
[10] T. Mohana Priya, Dr. M. Punithavalli & Dr. R. Rajesh Kanna, Machine Learning Algorithm for Development of Enhanced Support Vector Machine Technique to Predict Stress, Global Journal of Computer Science and Technology: C Software & Data Engineering, Volume 20, Issue 2, No. 2020, pp 12-20
[11] Ganesh Kumar and P.Vasanth Sena, "Novel Artificial Neural Networks and Logistic Approach for Detecting Credit Card Deceit," International Journal of Computer Science and Network Security, Vol. 15, issue 9, Sep. 2015, pp. 222-234
[12] Gyusoo Kim and Seulgi Lee, "2014 Payment Research", Bank of Korea, Vol. 2015, No. 1, Jan. 2015.
[13] Chengwei Liu, Yixiang Chan, Syed Hasnain Alam Kazmi, Hao Fu, "Financial Fraud Detection Model: Based on Random Forest," International Journal of Economics and Finance, Vol. 7, Issue. 7, pp. 178-188, 2015.
[14] Hitesh D. Bambhava, Prof. Jayeshkumar Pitroda, Prof. Jaydev J. Bhavsar (2013), "A Comparative Study on Bamboo Scaffolding And Metal Scaffolding in Construction Industry Using Statistical Methods", International Journal of Engineering Trends and Technology (IJETT) – Volume 4, Issue 6, June 2013, Pg.2330-2337.
[15] P. Ganesh Prabhu, D. Ambika, "Study on Behaviour of Workers in Construction Industry to Improve Production Efficiency", International Journal of Civil, Structural, Environmental and Infrastructure Engineering Research and Development (IJCSEIERD), Vol. 3, Issue 1, Mar 2013, 59-66.