

Medical Records Management Using Blockchain

BLOCKCHAIN TECHNOLOGY

Mini Project Submitted by

DIKSHA KALAMBE(BCA55)

OM PHARATE (BCA61)

HARSHAL PATIL (BCA63)

SURAJ TAPKIR (BCA64)

FOURTH

YEAR COMPUTER ENGINEERING



Department of Computer Engineering International
Institute of Information Technology Hinjawadi,
Pune – 411057

SEMESTER I (AY 2025-26)

TABLE OF CONTENTS

	TITLE	PAGE NO.
1.	ABSTRACT	1
2.	INTRODUCTION	2
2.1.	OBJECTIVE	3
2.2.	SCOPE	4
2.3.	SYSTEM ANALYSIS	6
2.3.1.	PROBLEM STATEMENT	
2.3.2.	PROPOSED SOLUTION	
2.3.3.	SOFTWARE AND HARDWARE DETAILS	
2.4.	IMPLEMENTATION	8
2.4.1.	PROJECT SETUP	
2.4.2.	EXECUTION STEPS	
3.	OUTPUT	9
4.	CONCLUSION	13
5.	REFERENCES	14

Abstract

Healthcare organizations handle large amounts of sensitive patient data, including personal details, medical history, prescriptions, lab reports, and diagnoses. Traditional centralized databases are vulnerable to security breaches, unauthorized modifications, and accidental data loss.

This project presents a **blockchain-based medical records management system** that ensures **data security, immutability, transparency, and auditability**. Each patient record is stored as a block containing detailed patient and doctor information. Blocks are cryptographically linked, forming an immutable chain that prevents unauthorized tampering.

The system also provides a web-based interface for healthcare staff to add, update, and view patient records efficiently. Tamper simulation and chain validation features provide an educational demonstration of blockchain principles in a real-world healthcare scenario.

This solution emphasizes how blockchain can transform healthcare data management by enhancing security, trust, and transparency.

INTRODUCTION

The healthcare industry generates large volumes of sensitive patient information every day. Mismanagement of this data can lead to serious consequences, including misdiagnosis, privacy breaches, and loss of trust.

Centralized databases traditionally used in hospitals are prone to vulnerabilities such as:

- **Unauthorized access:** Hackers or insider threats can access or modify patient records.
- **Tampering:** Data can be altered without traceability.
- **Data loss:** System failures can lead to permanent loss of medical records.

Blockchain technology addresses these issues by creating a **distributed, immutable ledger** of records:

- **Cryptographic Hashing:** Each block's content is hashed; any change alters the hash.
- **Immutability:** Previous blocks cannot be changed without altering the entire chain.
- **Traceability:** Every update or tampering attempt can be tracked and logged.

This project implements a **Medical Records Blockchain System** using Python and Flask. It provides a **secure, user-friendly, and interactive interface** to manage patient records and demonstrates the practical benefits of blockchain in healthcare.

OBJECTIVE

- **Secure Storage:** Implement a tamper-proof system to store sensitive medical data.
- **Data Integrity:** Ensure that all patient records are immutable once added to the blockchain.
- **Audit Trail:** Maintain a detailed log of all updates, tampering attempts, and access.
- **Transparency:** Provide visibility into the entire history of patient records.
- **User-Friendly Interface:** Build a web application to simplify record management for hospital staff.
- **Educational Demonstration:** Show blockchain concepts like hashing, immutability, and chain validation in action.

SCOPE

1. Healthcare Institutions:

Hospitals, clinics, and diagnostic centers can implement this blockchain system to securely store and manage patient medical records. Each patient's information—such as diagnoses, prescriptions, and lab reports—is stored in immutable blocks, ensuring that records cannot be altered without trace. This system enhances trust between patients and healthcare providers while streamlining record-keeping and reducing administrative errors.

2. Corporate Healthcare / Insurance Use:

Health insurance companies, corporate wellness programs, and occupational health departments can adopt the system to maintain secure, auditable records of employee medical histories, claim information, and treatment approvals. Decentralized record management ensures that insurance claims are transparent, tamper-proof, and easily verifiable, reducing fraud and improving efficiency.

3. Government and Public Health Applications:

At a larger scale, government health agencies can leverage the blockchain for nationwide patient record management, vaccination tracking, epidemic monitoring, or public health audits. By integrating with national digital identity systems, such as Aadhaar or other secure KYC solutions, the system can provide a traceable yet privacy-preserving record of patient interactions, ensuring accountability and reducing data misuse.

4. Technological Expansion:

- **Auditability & Logging:** Detailed logging of all access, updates, and tampering attempts to ensure accountability and regulatory compliance.
- **Privacy-Preserving Mechanisms:** Using advanced cryptographic techniques like Zero-Knowledge Proofs (ZKP) to ensure that sensitive patient data remains confidential while still being verifiable by authorized personnel.

5. Future Enhancements:

- Integration with hospital management systems and patient portals.
- Multi-user authentication with role-based access.
- Cloud-based blockchain for distributed access.
- Support for medical images, lab results, and large datasets.
- Real-time blockchain updates across multiple hospitals.
- AI integration for predictive healthcare insights using blockchain-secured data.

6. Research and Educational Scope:

The project serves as a valuable learning resource for blockchain developers, cybersecurity researchers, and students studying distributed ledger technologies. It provides hands-on experience in smart contract development, blockchain deployment, and decentralized user interface creation.

2.3 SYSTEM ANALYSIS

PROBLEM STATEMENT

Managing and securing medical records is a major challenge due to risks of data tampering, unauthorized access, and lack of transparency. Traditional centralized databases are vulnerable to manipulation and breaches. There is a need for a system that ensures data integrity, authenticity, and traceability of medical records. This project proposes a blockchain-based solution to securely store, verify, and monitor patient records using cryptographic hashing and decentralized validation.

PROPOSED SOLUTION

The proposed solution is a **Blockchain-Based Medical Record Management System**, where each new patient record is stored as a **block** in a blockchain. Once added, these blocks become immutable — preventing unauthorized edits or deletions. Any modification (such as record update or tampering attempt) is automatically detected due to cryptographic hashing and block verification mechanisms.

The system is built using **Python (Flask)** for backend blockchain logic and **HTML/CSS/JavaScript** for a simple and interactive web interface. Each record addition, tampering, or update event is logged for traceability.

System Workflow

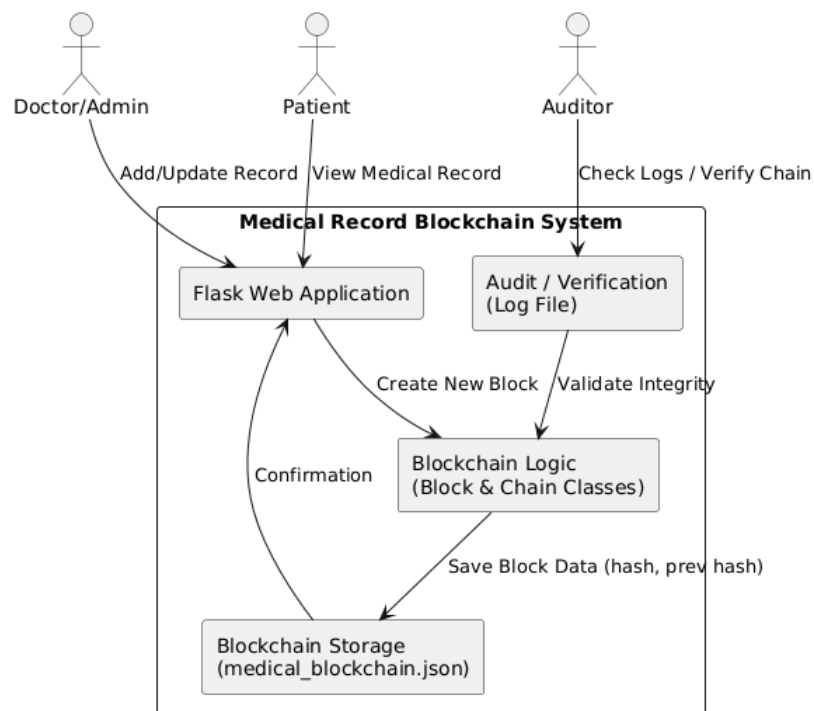


Fig. Medical Records Management Using Blockchain

SOFTWARE AND HARDWARE DETAILS

Software Requirements

Operating System:

Windows 10/11, macOS, or Linux

Backend Framework:

Python Flask (for web interface and server logic)

Blockchain Implementation:

Custom blockchain built using Python (JSON-based storage for immutable medical records)

Database / File System:

Local JSON file (medical_blockchain.json) used as the blockchain ledger

Browser:

Any modern browser (Chrome, Edge, Firefox) for accessing the Flask web app

IDE / Editor:

VS Code / PyCharm / Sublime Text

Hardware Requirements

Processor:

Intel Core i3 or higher / AMD Ryzen 3 or higher

RAM:

Minimum 4 GB (8 GB recommended for faster local testing)

Storage:

At least 1 GB free space for blockchain data and logs

Network Requirements:

Localhost or LAN access (optional for multi-node simulation)

Display:

Standard HD resolution (1366x768 or above)

2.4 IMPLEMENTATION

2.4.1 PROJECT SETUP

- Install dependencies: pip install flask
- Run the application: python app.py
- Open the web interface in a browser: <http://127.0.0.1:5000>
- Blockchain data is stored locally in **medical_blockchain.json**
- Audit logs of tampering or updates are saved in **blockchain_audit.log**
- Each block contains patient details, doctor information, and record type (Diagnosis / Prescription / Lab Report)

2.4.2 EXECUTION STEPS

- User launches the **Medical Records Blockchain** web application.
- Application initializes and loads existing blockchain data.
- Admin or Doctor enters patient and record details through the form.
- System hashes the Patient ID for privacy and creates a new block.
- The new block is linked to the previous block using SHA-256 hash.
- Blockchain validity is checked automatically after each transaction.
- Admin can simulate **Tamper** or **Update** actions for testing integrity.
- Any tampering or modification is detected and highlighted on the dashboard.
- Audit logs record user actions, timestamps, and old/new data for transparency.

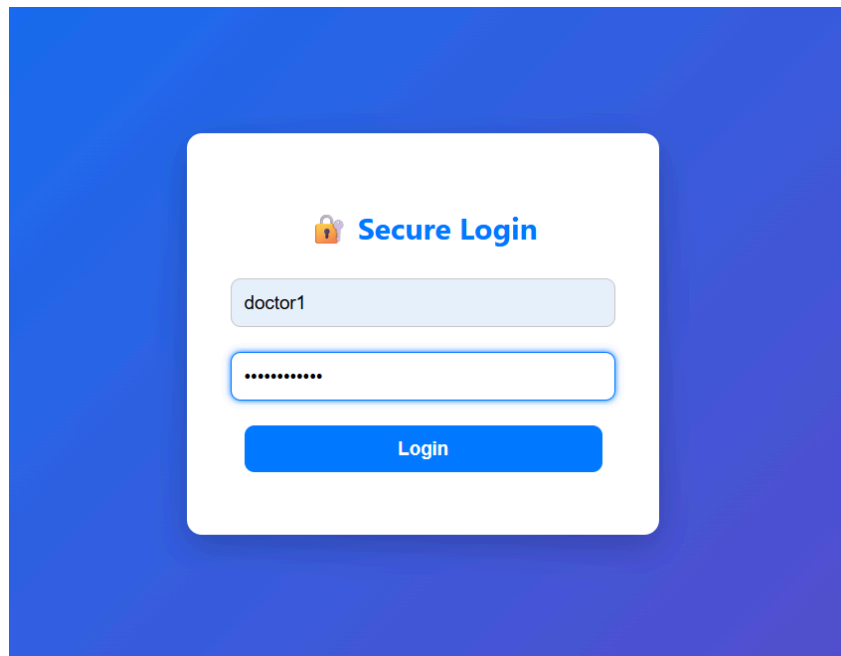
3. OUTPUT

The **Medical Records Blockchain System** successfully records, secures, and verifies patient medical data using blockchain technology. The system ensures that every record added is cryptographically linked, making it tamper-proof and transparent. The web-based interface displays real-time updates of the blockchain, helping users visualize the chain's integrity and detect any unauthorized changes.

Flask provides the interactive web UI, while SHA-256 hashing guarantees data immutability. Any tampering or updates are logged and visually marked, ensuring full traceability and accountability of all medical records.

Test Results:

- Successful Login
- Successful addition of new patient and doctor records.
- Verified cryptographic linking between blocks (hash and previous hash).
- Detected and logged any tampering or unauthorized data modification.
- Verified audit log entries for all updates and changes.
- Confirmed real-time display of valid and tampered block status on the dashboard.
- Ensured blockchain integrity validation after every transaction.



• *Figure 1. Successful Login*



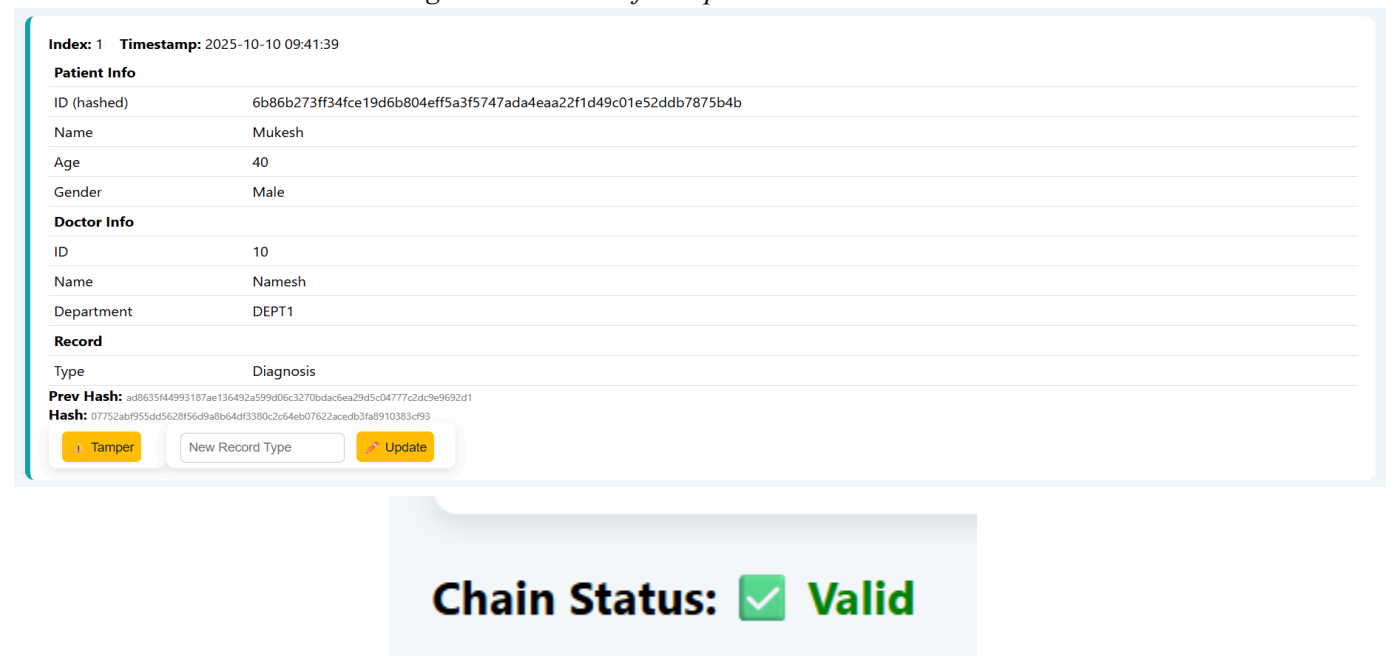
Medical Records Blockchain doctor1 Logout

Add New Medical Record

1 Mukesh 40 Male 10 Namesh DEPT1

Diagnosis Add Record

Figure 2. addition of new patient and doctor records.



Index: 1 Timestamp: 2025-10-10 09:41:39

Patient Info

ID (hashed)	6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
Name	Mukesh
Age	40
Gender	Male

Doctor Info

ID	10
Name	Namesh
Department	DEPT1

Record

Type	Diagnosis
------	-----------

Prev Hash: ad8635f44993187ae136492a599d06c3270bdac6ea29d5c04777c2dc9e9692d1
Hash: 07752abf955dd5628f56d9a8b64d3380c2c64eb07622acedb3fa8910383c93

Tamper New Record Type Update


Chain Status:  Valid

Figure 3. Verified cryptographic linking between blocks (hash and previous hash).

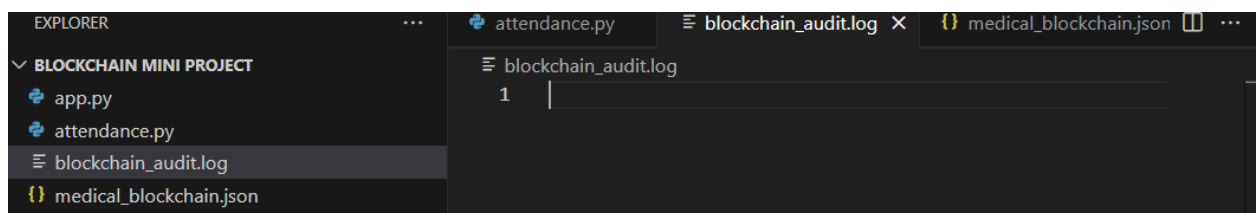


Figure 4. Detected and logged any tampering or unauthorized data modification.

Index: 1 **Timestamp:** 2025-10-10 09:41:39

Patient Info	
ID (hashed)	6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
Name	Mukesh
Age	40
Gender	Male
Doctor Info	
ID	10
Name	Namesh
Department	DEPT1
Record	
Type	Diagnosis

Prev Hash: ad8635f44993187ae136492a599d06c3270bdac6ea29d5c04777c2dc9e9692d1
Hash: 07752abf955dd5628f56d9a8b64df3380c2c64eb07622acedb3fa8910383cf93

Tamper

Fever

Update

Chain Status: ❌ Tampering Detected

Figure 5. if Someone tries to modify or temper

```
Welcome  attendance.py  blockchain_audit.log  medical_blockchain.json
blockchain_audit.log
1  [2025-10-10 09:55:03] User: doctor1 | Block: 1 | Action: Update | Old: {'patient_id': '6b8
2  [2025-10-10 09:55:37] User: doctor1 | Block: 1 | Action: Tamper | Old: Fever | New: Tamper
3
```

Figure 5. logging and chain status

4. CONCLUSION

Blockchain-Based Medical Records Management System demonstrates how blockchain technology can revolutionize healthcare data handling by introducing immutability, transparency, and security. By leveraging a decentralized ledger, this system eliminates the need for a single central authority, ensuring that medical records cannot be altered or deleted without detection.

Thus, this project effectively demonstrates the potential of blockchain technology in transforming healthcare record management into a secure, auditable, and transparent process, paving the way for more trustworthy digital healthcare systems in the future.

5. REFERENCES

1. Python Official Documentation

<https://docs.python.org/3/>

Reference for Python syntax, modules, and JSON/file handling used in implementing blockchain and Flask backend.

2. Flask Framework Documentation

<https://flask.palletsprojects.com/>

Official guide to Flask web framework, covering routes, templates, and request handling for building the web interface of the medical blockchain system.

3. Hashlib Module Documentation (Python Standard Library)

<https://docs.python.org/3/library/hashlib.html>

Explains the SHA-256 hashing algorithm used for block and patient ID encryption in the blockchain.

4. Zyskind, G., Nathan, O., & Pentland, A. (2015).

Decentralizing Privacy: Using Blockchain to Protect Personal Data.

2015 IEEE Security and Privacy Workshops (SPW), IEEE.

DOI: 10.1109/SPW.2015.27

Discusses the concept of decentralized data storage and privacy — a foundation for secure handling of patient medical records.

6. Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018).

Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology.

Sustainable Cities and Society, 39, 283–297.

DOI: 10.1016/j.scs.2018.02.014

Presents blockchain applications in healthcare for secure record sharing — relevant to this project's aim of tamper detection in medical data.

7. Mettler, M. (2016).

Blockchain technology in healthcare: The revolution starts here.

2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), IEEE.

