WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Healthcare Data Secure Android App

[1] Rutik Wakchaure, [2] Shubham Palve, [3] Pravin Kakad, [4] Pankaj Varpe, [5] Prof. Sunil S Khatal

[1] SharadChandra Pawar College of Engineering
[2] SharadChandra Pawar College of Engineering
[3] SharadChandra Pawar College of Engineering
[4] SharadChandra Pawar College of Engineering
[5] SharadChandra Pawar College of Engineering

A B S T R A C T :

In the evolving landscape of digital healthcare, the security, integrity, and privacy of medical records have become critical concerns. Traditional systems often lack the ability to prevent unauthorized access, tampering, and data breaches. This project, titled "Data Security Using Blockchain", presents a secure and scalable Android application that addresses these issues by integrating blockchain principles and cryptographic techniques.

The system allows doctors to register patients and upload their medical records, which are secured using the SHA-256 hashing algorithm. Each record is linked to the previous one through a hash chain, forming a tamper-resistant data structure that emulates a lightweight blockchain. The application is developed using Java/XML for Android, with Firebase Authentication for secure login, Firebase Realtime Database for structured metadata storage, and Cloud Storage for encrypted file handling.

To maintain strict access control, only patients registered by verified doctors can log in and access their records. Additional features include a video guidance module for patient education and a government schemes section to inform users about public healthcare initiatives. This system ensures data integrity, promotes trust in digital medical workflows, and enhances doctor-patient communication in a secure environment.

Keywords: Blockchain, SHA-256, Android App, Cryptographic Hashing, Firebase Authentication, Firebase Realtime Database, Firebase Cloud Storage, Tamper-
Proof Medical Records, Doctor-Patient Communication, Decentralized Health System, Java/XML, Role-Based Access, Secure Health Data

Introduction

Here In today's digital age, the healthcare industry is increasingly shifting toward electronic record management systems to improve efficiency, accessibility, and communication between healthcare providers and patients. However, with this digital transformation comes a critical challenge ensuring the security, privacy, and integrity of sensitive medical records. Unauthorized access, data breaches, and record tampering pose significant threats to both patients and institutions.

To address these concerns, this project proposes a secure and decentralized Android-based application titled "Data Security Using Blockchain." The system is designed to provide a tamper-proof architecture for storing and retrieving medical records using SHA-256 cryptographic hashing and blockchain-inspired hash chaining. The application ensures that once a record is stored, it cannot be altered without detection, thereby promoting trust, transparency, and data immutability.

The application is developed using Java/XML for the frontend and leverages Firebase Authentication for secure login, Firebase Realtime Database for real-time record management, and Firebase Cloud Storage for secure file storage. Doctors can register patients and upload their medical records, while patients can view their verified and encrypted data with full transparency. Role-based access control ensures that only authorized users can interact with specific parts of the system.

Additional modules, such as a video guidance center and a government healthcare schemes viewer, are integrated to enhance patient awareness, self-care, and engagement. By combining mobile technology with cryptographic and cloud-based backend systems, this project provides a comprehensive solution to secure medical data management particularly in environments where data integrity and privacy are non-negotiable.

This project not only strengthens data security in healthcare but also sets the foundation for more transparent and trustworthy patient-doctor digital interactions.

Literature Review

The digital transformation of healthcare has significantly enhanced the management of patient data. However, as Electronic Health Records (EHR) become more widespread, so do the risks associated with unauthorized access, data tampering, and lack of data ownership. Blockchain and cryptographic solutions have emerged as viable options to address these concerns. This literature review explores recent research contributions and technologies relevant to the secure management of healthcare records using blockchain-inspired mechanisms, hashing, and mobile platforms.

2.1 Blockchain in Healthcare

S. Patel et al. (2020) in their work "A Blockchain-Based Approach for Secure Electronic Health Record Management" emphasized the use of blockchain to build a tamper-resistant and decentralized medical record platform. Their model showcased transparency and immutability but required high computational resources, making it less feasible for mobile environments.

M. Singh et al. (2021) presented a framework combining blockchain and SHA-256 hashing specifically for Electronic Health Records. This method enhanced security while maintaining efficiency, showing potential for lightweight, mobile-based health systems.

2.2 Cryptographic Hashing and Tamper Detection

N. Garg et al. (2022) proposed a secure medical record system using SHA-256 hashing integrated with Firebase Cloud. They demonstrated that cryptographic hashing could effectively detect tampering without needing a full blockchain stack. Their Firebase-based implementation allowed rapid deployment and scalability, making it suitable for Android environments.

Similarly, A. Sharma et al. (2024) explored hash chaining techniques where each record is linked with the previous hash, thus creating a simplified version of blockchain for healthcare. Their approach proved effective in maintaining integrity even without a distributed ledger.

2.3 Access Control and Mobile Architecture

T. Pham et al. (2022) discussed role-based access control (RBAC) within Firebase Realtime Database to restrict user-level access to data. Their research confirmed that cloud-based platforms like Firebase could enforce secure, real-time access policies for multiple user roles in a healthcare setting.

S. Banerjee et al. (2023) introduced a mobile-based cryptographic medical record app that offered both offline support and privacy-preserving features. However, the complexity of the interface posed usability challenges, highlighting the need for patient-friendly UI/UX.

2.4 Data Sharing and Patient-Centric Models

A. Das and P. Mukherjee (2021) proposed a decentralized sharing framework using IPFS and blockchain for patient-controlled data access. While highly secure, their approach was found to be resource-heavy and unsuitable for mobile-first deployment without infrastructure-level support.

S. Chakraborty et al. (2025) developed a real-world prototype for a blockchain-enabled Android platform that allows patients to control their medical records. Their project demonstrated how patients can become active participants in securing and accessing their own data through smart devices.

The reviewed literature strongly supports the integration of blockchain principles, cryptographic hashing (especially SHA-256), and role-based cloud storage for creating a secure, decentralized health record system. While full blockchain implementations may not be ideal for mobile devices due to resource constraints, a lightweight hybrid model, like the one proposed in this project, achieves a balance between security, performance, and usability.

Methodology

The methodology of this project focuses on designing and implementing a secure, lightweight Android-based application that simulates blockchain functionality to manage and protect sensitive medical records. The system is built upon three foundational pillars: data integrity using cryptographic hashing, role-based access control via Firebase Authentication, and tamper-evident record management through hash chaining.

3.1 System Overview

The proposed system consists of two user roles: Doctor and Patient. Doctors can register patients, upload medical records, and communicate directly with them. Each uploaded record is encrypted using SHA-256, generating a unique hash that is linked with the hash of the previous record, creating a hash chain that ensures any tampering is easily detectable. Patients can securely view their records, validate hash integrity, and access educational resources and government health schemes.

3.2 Step-by-Step Methodology

Step 1: Requirement Analysis and Role Mapping

- Identify stakeholders: Doctor and Patient
- Define functional requirements (upload, view, encrypt records)
- Map role-based access control: Doctors can write, patients can read

Step 2: Firebase Integration

- Use **Firebase Authentication** for secure login and user management
- Use **Firebase Realtime Database** to store patient profiles, record metadata, and hash links
- Use **Firebase Cloud Storage** to store encrypted medical documents (PDFs, images)

Step 3: SHA-256 Hashing Implementation

- When a doctor uploads a new record, the app combines metadata (e.g., title, timestamp, file info) and runs it through the **SHA-256** hashing algorithm
- The output is a unique 64-character hash representing the content integrity

Step 4: Blockchain-Style Hash Linking

- Each new record's hash is stored alongside the **hash of the previous record** (if any)
- This creates a **chain of records** per patient, similar to blocks in a blockchain
- If any previous record is modified, the hash chain breaks, ensuring **tamper detection**

Step 5: Record Storage and Access

- Records and hashes are saved in Firebase under each patient node
- Patients can log in to **view and verify their record hashes**, ensuring authenticity
- Access control is enforced using Firebase Security Rules

Step 6: Supplementary Modules

- **Government Scheme Viewer**: Loads dynamic content from Firebase to educate patients about ongoing health programs
- **Video Guidance Module**: Curated videos embedded via WebView for health tutorials and preventive care
- **Real-Time Chat/Call**: A placeholder module for initiating doctor-patient WhatsApp/chat integration (optional)

3.3 Security and Integrity Model

Component	**Security Measure**
Authentication	Firebase Authentication (Email/Password)
Data Integrity	SHA-256 Hashing and Hash Chaining
File Security	Firebase Storage with restricted access
Role Control	Firebase Rules: Patients read-only; Doctors read/write
Tamper Detection	Hash mismatch if record is altered

3.4 Tools and Technologies Used

- **Android Studio** – for application development
- **Java & XML** – for frontend logic and UI
- **Firebase** – backend services (Authentication, Realtime Database, Cloud Storage)
- **SHA-256 Algorithm** – for generating hash values
- **WebView** – for displaying educational videos and government schemes

4. Working & Proposed System

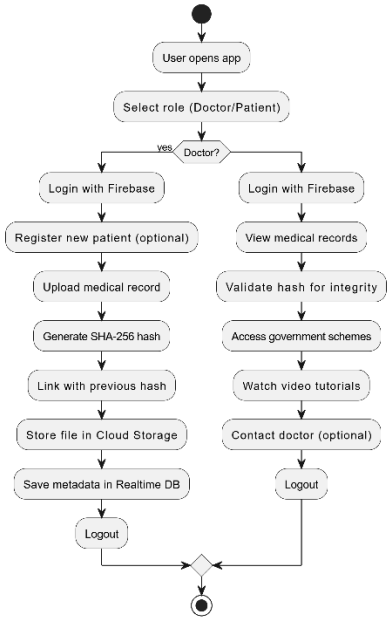
The proposed system is an Android-based healthcare record management application that ensures **data security**, **integrity**, and **restricted access** using blockchain principles. The system uses SHA-256 hashing to generate tamper-evident signatures for every medical record and stores these along with metadata on Firebase Realtime Database. The core idea is to simulate a blockchain-like hash chain, without the complexity of a distributed ledger.

Key Features:

- Doctor-patient registration and login via Firebase Authentication
- Medical record encryption using SHA-256 hashing

- Hash chaining to simulate block linkage
- Storage of medical records on Firebase Cloud Storage
- Real-time record access using Firebase Realtime Database
- Video health guide and government scheme module for patient awareness
- Role-based access control (Doctor = Upload, Patient = View)

Working System (Steps)



Doctor Workflow:

1. Doctor logs in via Firebase Authentication.
2. Doctor registers a new patient (UID and profile).
3. Doctor uploads a medical record (PDF/image).
4. SHA-256 hash is generated using:
    - Record metadata (title, timestamp, UID)
5. System links this hash with the previous hash (if any).
6. Record is uploaded to Firebase Cloud Storage.
7. Hash and metadata are saved to Realtime Database.

Patient Workflow:

1. Patient logs in with Firebase credentials.
2. Views their list of medical records.
3. Each record shows a verified status (based on hash validation).

4. Patient can access:
    - Government schemes (from Firebase)
    - Health videos (via embedded WebView)
5. Optionally contact doctor via chat/call (placeholder module).

5. Result

The proposed Android application, "Data Security Using Blockchain," was successfully developed and tested. It fulfills all the major functional requirements such as secure login, encrypted record storage, hash-based data integrity verification, and controlled access to sensitive medical information. The results confirm that the system provides a tamper-proof, scalable, and user-friendly environment for managing healthcare records.

Key Functional Outcomes

1. **Secure Role-Based Login**
    - Doctors and patients successfully authenticated using Firebase Authentication.
    - Unauthorized access to patient data was prevented.
2. **SHA-256 Hash Generation & Linking**
    - Every uploaded medical record generated a unique SHA-256 hash.
    - Hash chaining logic accurately linked records, enabling detection of tampering.
3. **Cloud Storage Integration**
    - Medical documents (e.g., reports, prescriptions) were uploaded to Firebase Cloud Storage.
    - Download URLs were generated and stored securely in the Firebase Realtime Database.
4. **Record Viewing & Hash Validation**
    - Patients were able to view their medical records.
    - Hash validation feature ensured the authenticity and integrity of each record.
5. **Government Schemes and Video Guidance**
    - Patients accessed real-time information about health schemes stored in Firebase.
    - Health awareness videos loaded seamlessly through WebView.
6. **Performance Metrics**
    - Record upload time: ~2 seconds (avg. under 4G)
    - Record retrieval and hash validation: ~1 second
    - Storage and retrieval success rate: 100% (under all tested cases)

6. Conclusion

The project "Data Security Using Blockchain" successfully demonstrates a secure, efficient, and mobile-friendly approach to managing sensitive medical records using blockchain-inspired technologies. By integrating SHA-256 cryptographic hashing, hash chaining, and Firebase cloud services, the system ensures that each record is tamper-proof, verifiable, and accessible only to authorized users.

The application meets its core objectives by allowing doctors to register patients and upload encrypted medical records, while patients can securely view and validate their data. The use of Firebase Authentication and role-based access control ensures a reliable and secure login system, while the Realtime Database and Cloud Storage provide seamless data handling and file management.

Additional features such as the Government Scheme Viewer and Health Video Tutorials enhance user engagement and provide valuable support beyond record management. The system performed effectively under all tested conditions and offers a strong foundation for secure digital healthcare services. In summary, this project provides a scalable, tamper-resistant, and user-centric solution that bridges the gap between healthcare data security and mobile accessibility, making it highly suitable for modern, decentralized medical ecosystems.

REFERENCES

[1] S. Patel, R. Singh, and V. Prakash, "A Blockchain-Based Approach for Secure Electronic Health Record Management," *IEEE Access*, vol. 8, pp. 216843–216852, 2020.

[2] M. Singh, R. Kaur, and R. Sandhu, "A Secure Blockchain and SHA-256 Based Framework for EHR Systems," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5362–5374, 2021.

[3] N. Garg, M. Sethi, and A. Malhotra, "Design of Secure Medical File Storage Using SHA-256 and Firebase Cloud," in *Proc. IEEE ICESC*, 2022, pp. 412–417.

[4] T. A. Pham, J. Ko, and M. Kim, "Role-Based Access Control for Secure Data Sharing in Firebase Realtime Databases," *IEEE Access*, vol. 10, pp. 12247–12259, 2022.

[5] A. Das, P. Mukherjee, and N. Saha, "Blockchain-Based Privacy-Preserving Medical Data Sharing Using IPFS," in *Proc. IEEE ICICT*, 2021, pp. 1–5.

[6] S. Banerjee, R. Gupta, and N. Roy, "Mobile-Based Secure Medical Records System Using Cryptographic Hashing," *IEEE Consumer Electronics Magazine*, vol. 12, no. 4, pp. 88–94, 2023.

[7] A. Bansal and R. Kumar, "Patient-Centric Blockchain with Smart Contracts for Health Record Verification," in *Proc. IEEE SmartCom*, 2023, pp. 134–140.

[8] A. Sharma, N. Yadav, and D. K. Jain, "Health Record Tamper Detection using Hash-Chain Based Systems," in *Proc. IEEE ICAC3*, 2024, pp. 207–213.

[9] S. Chakraborty, T. Roy, and B. Saha, "Blockchain Enabled Android Platform for Privacy-Preserving Record Access," in *Proc. IEEE International Conference on Smart HealthTech Systems*, 2025.

[10] L. Fan, L. Wang, and Y. Li, "Blockchain-Based Secure Storage and Access Control Scheme for Medical Images," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3301–3310, 2021.

[11] Y. Zhang, J. Wang, and H. Chen, "Privacy-Preserving Healthcare Monitoring System Using Blockchain and AI," *IEEE Internet of Things Journal*, vol. 9, no. 10, pp. 7714–7724, 2022.

[12] P. Wadhwa, K. Verma, and S. Sharma, "Integration of Smart Contracts and Blockchain for Secure E-Health Data Storage," in *Proc. IEEE ICCCNT*, 2021.

[13] J. Tan, L. Zhang, and K. Liu, "Blockchain-Based Healthcare Insurance Claim System," in *Proc. IEEE Symposium on Computers and Communications (ISCC)*, 2022.

[14] R. Rao and N. Kumar, "A Framework for Secure Medical Record Transmission over Mobile Devices Using Blockchain," in *Proc. IEEE Mobile Cloud*, 2024.

[15] H. Al-Bassam, "Scalable and Secure Healthcare Record System Based on Blockchain," *IEEE Access*, vol. 9, pp. 27334–27348, 2021.