IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

HealthChainSync Android App Using AI

[1] Swati Ravindra Patil, [2]Prof. Manoj V. Nikum, [3]Prof.Praveen I. Patil

[1]Student of Masters of Engineering, [2]Assistant Professor , [3]Assistant Professor

[1]Computer Science and Engineering,

[1]Shri Jaykumar Rawal Institute Of Technology, Dondaicha , India

Abstract: HealthChainSync is a secure Android-based health-record management application developed to improve the storage, sharing and verification of medical information between doctors and patients. The application is developed using Java and XML and provides separate Doctor and Patient interfaces. Firebase Authentication is used to verify users, while role-based access control restricts application functions according to the assigned user role.

Patients can upload prescriptions, diagnostic reports and other medical documents to Firebase Cloud Storage. User profiles, document metadata, medical-record details, doctor remarks and access permissions are maintained in Firebase Realtime Database. Authorized doctors can view permitted patient records, add medical remarks and update treatment-related information without gaining unrestricted access to the patient's account.

Index Terms - Android Application, Electronic Health Records, Firebase, Private Blockchain, SHA-256, Medical Data Integrity, Role-Based Access Control, Generative AI, NLP Chatbot, Healthcare Data Security.

Introduction

The rapid adoption of digital healthcare systems has increased the generation and exchange of electronic health records such as prescriptions, laboratory reports, diagnostic images and treatment summaries. These records help doctors access a patient's medical history quickly, but conventional centralized systems remain vulnerable to unauthorized access, accidental modification, data leakage and single-point failures. Patients may also have limited control over who can access their medical information.

HealthChainSync is an Android-based doctor–patient health-record management application designed to improve the security, accessibility and integrity of medical documents. The application is developed using Java and XML, with Firebase Authentication for identity verification, Firebase Cloud Storage for medical-file storage and Firebase Realtime Database for metadata, permissions, doctor remarks and user profiles. Separate Doctor and Patient roles are implemented using role-based access control.

The system follows a hybrid cloud–blockchain architecture. Large medical files are stored in Firebase Cloud Storage rather than directly inside the blockchain. Whenever a patient uploads a document, a SHA-256 hash is generated from the file bytes. This hash acts as a unique digital fingerprint of the document. The record identifier, patient identifier, timestamp, file hash and previous block hash are stored in a private blockchain ledger. During retrieval, the application recalculates the SHA-256 hash and compares it with the blockchain value. If both values match, the document is considered unchanged; otherwise, the system generates a possible-tampering warning.

Authorized doctors can view patient records, enter medical remarks and update treatment information according to the permissions granted by the patient or administrator. Any new version of a document generates a new hash and blockchain transaction instead of replacing the existing ledger entry.

HealthChainSync also integrates a Generative-AI-powered NLP chatbot for general health awareness, preventive-care guidance and symptom-related information. The chatbot does not provide a confirmed diagnosis, prescribe medicine or replace consultation with a qualified healthcare professional. Educational videos and official government healthcare-scheme information are provided through WebView integration.

I. LITERATURE REVIEW

1. Leonardo da Costa, Billy Pinheiro, Weverton Cordeiro, Roberto Araújo and Antônio Abelém presented "Sec-Health: A Blockchain-Based Protocol for Securing Health Records" in IEEE Access, vol. 11, 2023, pp. 16605–16620. The researchers proposed a blockchain-based protocol addressing confidentiality, integrity, anonymity, access control, revocation, interoperability and emergency access. Their proof-of-concept showed that blockchain and distributed storage could reduce health-record access time in specific scenarios while preserving auditability. The work supports HealthChainSync's use of an immutable ledger and role-based record access. However, the proposed protocol is comparatively complex, whereas HealthChainSync uses Firebase for practical mobile storage and a private ledger for integrity verification.

2. T. Haritha and A. Anitha published "Multi-Level Security in Healthcare by Integrating Lattice-Based Access Control and Blockchain-Based Smart Contracts System" in IEEE Access, vol. 11, 2023, pp. 114322–114340. The study integrated lattice-based access control with blockchain smart contracts to assign different security levels to healthcare users and resources. It demonstrated that access decisions can be enforced according to user roles and the confidentiality level of medical data. This work supports the Doctor and Patient role separation used in HealthChainSync. However, implementing full lattice-based security would increase computational and development complexity for a student-level Android system; therefore, HealthChainSync uses Firebase Security Rules and blockchain audit records.

3. Sangita Jaybhaye, Rutuja Desai, Gauri Choudhari, Isha Dashetwar and P. Dagale presented "HealthVault: A Blockchain-Based Patient Health Records Management System" at the 2024 IEEE 9th International Conference for Convergence in Technology. The authors developed a patient-oriented health-record management system using Ethereum, smart contracts and decentralized mechanisms. Their findings highlighted improved record immutability, transparency and patient control compared with conventional centralized databases. The study is directly related to HealthChainSync's patient-controlled access and ledger-based integrity verification. Its Ethereum implementation may introduce transaction costs and delays, while HealthChainSync proposes a permissioned private ledger suitable for a controlled doctor–patient environment.

4. Rashi Agrawal and Kanchan Patil presented "Blockchain Technology for Medical Records Security Using Fit Viability Approach" at the 2024 2nd International Conference on Advancement in Computation and Computer Technologies, pp. 805–810. The paper examined the technical and organizational suitability of blockchain for medical-record security. It found that blockchain can improve trust, traceability and integrity, but implementation depends on cost, infrastructure, user adoption and system compatibility. This finding supports the hybrid design of HealthChainSync, where Firebase provides practical mobile storage while blockchain is used only for hashes and verification data. This avoids placing large documents directly on the ledger.

5. Arjun Rajasekharan and Rani Koshy presented "EMRChain: Electronic Medical Records Management System Using Blockchain" at the 2024 IEEE International Conference on Blockchain and Distributed Systems Security, pp. 1–6. The system addressed the risks of conventional centralized EMR platforms by using blockchain for secure, transparent and decentralized record management. The research emphasized retaining large files outside the blockchain while keeping references, access information and verification data on the ledger. This architecture strongly supports HealthChainSync's

separation of Firebase file storage and blockchain hashes. It also demonstrates that blockchain should serve as an integrity and audit layer rather than an expensive large-file database.

6. V. Santhi, Diyaa Santhosh, N. Samyuktha and C. Sachitha presented "Blockchain-Enhanced Secure and Efficient IPFS-Based EHR Management: A Decentralized Approach" at the 2024 International Conference on Emerging Trends in Networks and Computer Communications. The study combined a consortium blockchain with IPFS to securely store and share electronic health records. Blockchain maintained tamper-resistant transaction details, while IPFS handled larger healthcare files. The findings show that separating the ledger from file storage improves scalability. HealthChainSync follows the same fundamental principle but uses Firebase Cloud Storage instead of IPFS to simplify Android integration, synchronization and user authentication.

7. Murat Kuzlu, Zhenxin Xiao, Salih Sarp, Ferhat Ozgur Catak, Necip Gurler and Ozgur Guler presented "The Rise of Generative Artificial Intelligence in Healthcare" at the 2023 12th Mediterranean Conference on Embedded Computing, pp. 1–4. The paper examined applications of Generative AI in medical imaging, drug discovery, documentation, patient engagement and healthcare assistance. It also identified risks involving inaccurate responses, privacy, bias, accountability and ethical use. These findings support the inclusion of an NLP chatbot in HealthChainSync, but they also justify restricting the chatbot to awareness and preventive guidance rather than diagnosis or treatment decisions.

8. Sara Montagna, Gianluca Aguzzi, Stefano Ferretti, Martino F. Pengo, Lorenz Cuno Klopfenstein, Michele Ungolo and Matteo Magnini presented "LLM-Based Solutions for Healthcare Chatbots: A Comparative Analysis" at the 2024 IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 346–351. The study examined LLM-based healthcare chatbots for chronic-disease self-management and compared externally hosted models with locally deployed models. The findings identified significant concerns regarding sensitive-data disclosure, reliability and difficulty controlling locally deployed models. HealthChainSync therefore limits the chatbot to general information, displays a medical disclaimer and should avoid transmitting identifiable medical records to the AI service without explicit consent.

II. METHODOLOGY

The proposed HealthChainSync system is developed as an Android application using Java and XML, with separate interfaces for Doctors and Patients. Users first register and log in through Firebase Authentication, while their profile details and assigned roles are stored in Firebase Realtime Database. After authentication, patients can upload prescriptions, diagnostic reports and other medical documents to Firebase Cloud Storage. During each upload, the application reads the file data and generates a unique SHA-256 hash that acts as the document's digital fingerprint.

The record ID, patient ID, timestamp, file hash, transaction type and previous block hash are stored as a new transaction in the private blockchain ledger. The file's storage reference, metadata and doctor-access permissions are maintained in Firebase Realtime Database. When a medical document is retrieved, the application downloads the file, recalculates its SHA-256 hash and compares it with the hash recorded in the blockchain. If both hashes match, the document is verified as unchanged; if they differ, the application displays a possible-tampering warning.

Authorized doctors can access patient records, add medical remarks and update treatment-related information according to role-based permissions. Any updated document is stored as a new version with a new hash and blockchain entry, preserving the original record history. The system also integrates a Generative-AI-powered NLP chatbot for general health awareness, symptom-related information and preventive-care guidance, along with educational videos and government healthcare-scheme information displayed through WebView.

III. BLOCK DIAGRAM

The HealthChainSync block diagram represents the interaction between the Patient, Doctor and Android application. Both users register and log in through Firebase Authentication, while their profiles and roles are maintained in Firebase Realtime Database. Patients can upload prescriptions, diagnostic reports and other medical documents through the Android application. The files are stored in Firebase Cloud Storage, whereas their metadata, access permissions and doctor remarks are stored in Firebase Realtime Database. Authorized doctors can view the patient's permitted medical records, add remarks and update treatment-related information.

Whenever a medical document is uploaded, the SHA-256 engine generates a unique digital fingerprint of the file. This hash, along with the record ID, patient ID, timestamp and previous block hash, is stored in the private blockchain ledger. During retrieval, the application recalculates the file hash and compares it with the blockchain value. A matching hash confirms that the document has not changed, while a mismatch generates a possible-tampering warning. The application also connects to a Generative AI-powered NLP chatbot for general health awareness and preventive-care guidance. Educational videos and official government healthcare-scheme information are displayed through the WebView-based healthcare-awareness module.

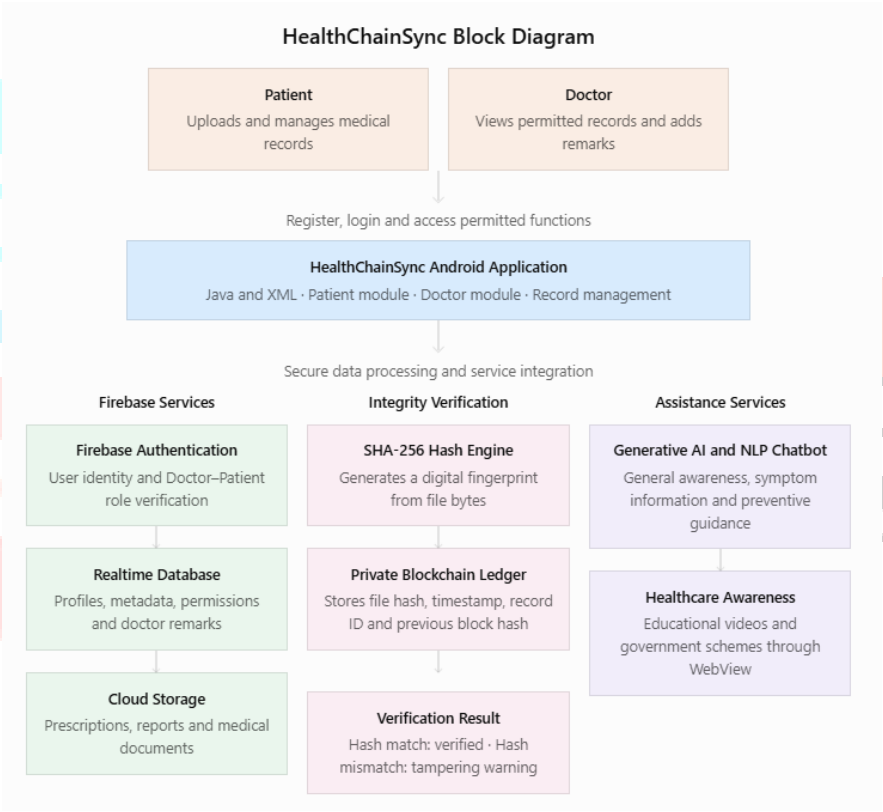

Fig 1 : Block Diagram

V. RESULTS AND DISCUSSION

The proposed HealthChainSync system theoretically provides a secure and organized method for managing digital medical records between doctors and patients. Firebase Authentication verifies users and separates Doctor and Patient access according to their assigned roles. Patients can upload prescriptions, diagnostic reports and other medical documents to Firebase Cloud Storage, while the associated metadata, permissions and doctor remarks are managed through Firebase Realtime Database. This separation provides efficient file storage and real-time data synchronization without placing large medical files directly inside the blockchain.

The SHA-256 and private blockchain modules provide integrity verification for uploaded medical records. A unique SHA-256 hash is generated for every file and stored in the blockchain with the record ID, patient ID, timestamp and previous block hash. When the file is retrieved, its hash is regenerated and compared with the blockchain value. A matching hash theoretically confirms that the file remains unchanged, while a mismatch indicates possible modification or corruption. However, SHA-256 does not encrypt the medical document;

confidentiality must still be maintained through Firebase Security Rules, secure communication and proper access control.

Result Analysis

Module	Result	Analysis
User Authentication	Valid users receive access according to their role	Prevents basic unauthorized access and separates Doctor and Patient functions
Medical-Record Upload	Files are stored successfully with their metadata	Cloud Storage handles files efficiently while Realtime Database manages record information
SHA-256 Hashing	A unique hash is generated for every file version	Even a minor file change produces a different hash
Blockchain Ledger	Hash and transaction information remain linked chronologically	Provides traceability and makes ledger modification detectable
Integrity Verification	Original files produce matching hashes	Hash match verifies consistency; mismatch generates a tampering warning
Doctor Access Control	Only permitted doctors can view records and add remarks	Protects patient information through role and permission checks
AI and Awareness Module	Users receive general health information and educational content	Improves awareness but must not be treated as medical diagnosis

The table shows the expected results of the major HealthChainSync modules. The authentication and access-control modules ensure that patients and doctors can access only the functions permitted for their roles. The medical-record module stores large documents in Firebase Cloud Storage and keeps their metadata separately in Firebase Realtime Database, improving storage efficiency and data organization.

The SHA-256 and blockchain modules form the main security mechanism. Every uploaded file generates a unique hash, which is recorded in the private blockchain. If the file remains unchanged, the regenerated hash matches the stored value. If the document is edited, replaced or corrupted, the new hash becomes different and the application displays an integrity-verification failure. The AI chatbot and healthcare-awareness modules improve access to general information, but their output is advisory and not a replacement for professional medical consultation.

Discussion

The main advantage of HealthChainSync is its hybrid cloud–blockchain architecture. Firebase offers fast authentication, real-time synchronization and scalable document storage, while the private blockchain maintains an immutable record of file hashes and transactions. This approach is more practical than storing complete medical reports inside the blockchain, which would increase storage requirements and processing time.

The proposed system improves traceability because each blockchain entry contains the previous block hash. Consequently, changing an earlier transaction affects the hashes of subsequent blocks and makes manipulation detectable. Document updates should therefore be stored as new versions with new blockchain entries instead of replacing the original record. This preserves a chronological medical-record history.

VI. CONCLUSION

The HealthChainSync provides a secure Android-based platform for managing medical records between doctors and patients. The system combines Firebase Authentication, Realtime Database and Cloud Storage with SHA-256 hashing and a private blockchain ledger. This architecture enables patients to upload and manage medical documents while allowing authorized doctors to review records and add remarks according to role-based permissions.

The SHA-256 and blockchain mechanism detects whether a stored document has changed after its original registration. Generative AI and WebView modules improve access to general healthcare information, preventive-care guidance, educational videos and government healthcare schemes. However, the chatbot remains an informational assistant and does not replace qualified medical professionals.

The project demonstrates that cloud storage and blockchain do not need to compete. Firebase can efficiently manage application data and files, while blockchain provides a separate, tamper-evident verification and audit layer. Future enhancements can include document encryption, digital signatures, multi-factor authentication, emergency access, consent expiry, blockchain-node distribution and privacy-preserving AI integration.

IV. ACKNOWLEDGMENT

We sincerely thank our project guide, faculty members and institution for their valuable guidance and support throughout this project. We also acknowledge our team members, friends and family for their continuous encouragement and assistance in completing the HealthChainSync project successfully.

REFERENCES

1] L. da Costa, B. Pinheiro, W. Cordeiro, R. Araújo and A. Abelém, "Sec-Health: A Blockchain-Based Protocol for Securing Health Records," *IEEE Access*, vol. 11, pp. 16605–16620, 2023, doi: 10.1109/ACCESS.2023.3245046.

[2] T. Haritha and A. Anitha, "Multi-Level Security in Healthcare by Integrating Lattice-Based Access Control and Blockchain-Based Smart Contracts System," *IEEE Access*, vol. 11, pp. 114322–114340, 2023, doi: 10.1109/ACCESS.2023.3324740.

[3] S. Jaybhaye, R. Desai, G. Choudhari, I. Dashetwar and P. Dagale, "HealthVault: A Blockchain-Based Patient Health Records Management System," in *2024 IEEE 9th International Conference for Convergence in Technology (I2CT)*, 2024, doi: 10.1109/I2CT61223.2024.10544145.

[4] R. Agrawal and K. P. Patil, "Blockchain Technology for Medical Records Security Using Fit Viability Approach," in *2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT)*, pp. 805–810, 2024, doi: 10.1109/InCACCT61598.2024.10551119.

[5] A. Rajasekharan and R. Koshy, "EMRChain: Electronic Medical Records Management System Using Blockchain," in *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, pp. 1–6, 2024, doi: 10.1109/ICBDS61829.2024.10837244.

[6] V. Santhi, D. Santhosh, N. Samyuktha and C. Sachitha, "Blockchain-Enhanced Secure and Efficient IPFS-Based EHR Management: A Decentralized Approach," in *2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, pp. 1–8, 2024, doi: 10.1109/ETNCC63262.2024.10767489.

[7] M. Kuzlu, Z. Xiao, S. Sarp, F. O. Catak, N. Gurler and O. Guler, "The Rise of Generative Artificial Intelligence in Healthcare," in *2023 12th Mediterranean Conference on Embedded Computing (MECO)*, pp. 1–4, 2023, doi: 10.1109/MECO58584.2023.10155107.

[8] S. Montagna, G. Aguzzi, S. Ferretti, M. F. Pengo, L. C. Klopfenstein, M. Ungolo and M. Magnini, "LLM-Based Solutions for Healthcare Chatbots: A Comparative Analysis," in *2024 IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events*, pp. 346–351, 2024, doi: 10.1109/PerComWorkshops59983.2024.10503257.

[9] M. Lakshmanan, G. S. Anandha Mala, G. Sivakumar, V. S. Divya Sundar, R. Kesavan and A. A. S. Jeena, "A Secure and Efficient Framework for Storing Medical Data Using Blockchain and Cloud Servers," in *2024 8th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, pp. 1661–1667, 2024, IEEE Xplore.

[10] D. N. Joy and C. S. Yadav, "Providing a Robust Blockchain-Based Framework for the Secure Transmission of EHRs Across the HIoT," in *2024 5th International Conference on Data Intelligence and Cognitive Informatics (ICDICI)*, pp. 158–165, 2024, doi: 10.1109/ICDICI62993.2024.10810894.
[11] P. Sivaprakash, R. M. Dilip Charaan, J. Vimala Ithayan, M. Sankar, R. Chithambaramani and D. Marichamy, "IPFS-Based Blockchain Enabled System for Secure Data Storage and Access in Healthcare," in *2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI)*, pp. 203–208, 2024, doi: 10.1109/ICoICI62503.2024.10696438.
[12] O. Chin, N. S. Jamil, Z. Zainudin, N. A. Hitam, N. Ibrahim and A. H. Ahmad Sa'ahiry, "OYEN: A User-Centric LLM-Based Bilingual Healthcare Chatbot," in *2024 5th International Conference on Artificial Intelligence and Data Sciences (AiDAS)*, pp. 435–440, 2024, doi: 10.1109/AiDAS63860.2024.10730140.
[13] A. Kapoor and S. D. Shetty, "Enhancing Healthcare Information Accessibility Through a Generative Medical Chatbot," in *2024 International Conference on Emerging Technologies in Computer Science for Interdisciplinary Applications (ICETCS)*, pp. 1–4, 2024, doi: 10.1109/ICETCS61022.2024.10543529.
[14] S. Akilesh, A. Sheik Abdullah, R. Abinaya, S. Dhanushkodi and R. Sekar, "A Novel AI-Based Chatbot Application for Personalized Medical Diagnosis and Review Using Large Language Models," in *2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE)*, pp. 1–5, 2023, doi: 10.1109/RMKMATE59243.2023.10368616.
[15] S. Sant and P. R. Bhaladhare, "Medical Data Security and Privacy Preservation Using Blockchain Technology Integrated With Healthcare 4.0 Standard: Current Methods and Challenges," in *2024 2nd DMIHER International Conference on Artificial Intelligence in Healthcare, Education and Industry*, 2024, IEEE Xplore.