REVOLUTIONIZING ELECTRONIC HEALTH RECORDS WITH BLOCKCHAIN SECURITY

[1*] Dr. B. Kiranmai, [1]Jurru Nirosha, [2]Nune Sujitha, [3]S Sarika, [4]Garlapati Vaishnavi
[1]Associate Professor, [1,2,3,4]Student
[1,2,3,4]Dept of CSE (Data Science)
Sreyas Institute of Engineering and Technology, Hyderabad

Abstract. Cloud Health Records usher in the major transformation in medicine, with digital recording and data sharing related to the patient and associated information. The patients and their families now enjoy a very limited ability to give or deny consent for the use of their health data.[5] Security breaches that arise mostly due to the third-party interveners and wherever will lead to privacy violations and lack of transparent access control, many countries compromising the laws or rights of the owner to privacy or legitimacy [1]. The proposed EHR model based on blockchain technology is decentralized and integrated with IPFS, Flask, MongoDB, and smart contracts. This architecture gives patients full rights over their health record, yet providing the possibilities of safe, auditable, and privacy-preserving data sharing [2]. In that system, all transactions related to grants, revocations, or uploads of records are immutably logged in the Ethereum chain [3]. Health records are stored on IPFS in encrypted form, while only metadata and permissions reside on the chain. Specified dynamic access rules are enforced by smart contracts to ensure ethical and compliant data management. Performance evaluation has shown that it is superior to legacy EHR systems with respect to confidentiality, scalability, and system trustworthiness [4].

Keywords: Electronic Health Records, Blockchain, IPFS, Flask, MongoDB, Ethereum, Smart Contracts, Data Privacy, Healthcare Security.

1 Introduction

Thus, digitizing health records is under way, and it is currently shifting from very basic protocols towards internet-based ones. By virtue of CHRs, a patient-provider nexus could function in real-time: patient information can be viewed or updated

simultaneously on both ends. Patient care constitutes prescribing, diagnosing, treatment history, investigations recorded in the laboratory, etc. Therefore, patient care carries the weight of diagnosing and clinical decision-making; CHRs provide ease of access and continuity of care but pose serious challenges pertaining to security, data privacy, and unauthorized access.

Most traditional EHR systems are subjected to centralized cloud architectures that make them susceptible to malicious security breaches, system failures, and unauthorized patient data manipulations. Patients have little opportunity to distinguish who accesses their records, leading to asymmetry of information and hence discontent towards the providers. Data officers are ever concerned in recent years about violations to data integrity, confidentiality, and consentability of the patient. With the advent of telemedicine, AI-based diagnosis, wearable devices for healthcare and other modes of healthcare, the risk of privacy breach equally so goes up, calling for a strong remedy.

This study proposes a blockchain-based Cloud Health Record management system to solve these issues. The decentralized, tamper-proof, and cryptographically secured nature of a blockchain scenario offers an alternative to the traditional EHR models. Combining the file storage capabilities of IPFS (InterPlanetary File System), with Flask and MongoDB for system interaction and indexing of data, the system allows patients to have full control over their records. Access to the records is controlled by smart contracts deployed on the Ethereum blockchain, and all transactions are recorded for auditability, which are immutable in nature. Thus, sensitive data are protected under this system, and the whole health infrastructure now regains the trust of the patient together with accountability and integrity that comes with ethical health.

1.1 Objective

The primary objective of this project would be the construction of a highly secure and decentralized cloud health record system while preserving patient data confidentiality, integrity, and availability. Hence, the initiative seeks to address some significant concerns that encompass unauthorized data access, insecure/free sharing of records across institutions, and limited patient control over their health information [1][2]. The model provided by blockchain and smart contracts provides superior access controls [3]. The project employs IPFS for file storage and Flask for web interaction to ensure ease of use, efficiency, and adherence to privacy, transparency, and user choice.

1.2 Scope

The design and development of a health record system will weigh heavy on decentralization, security, and user empowerment. The scope brings in blockchain

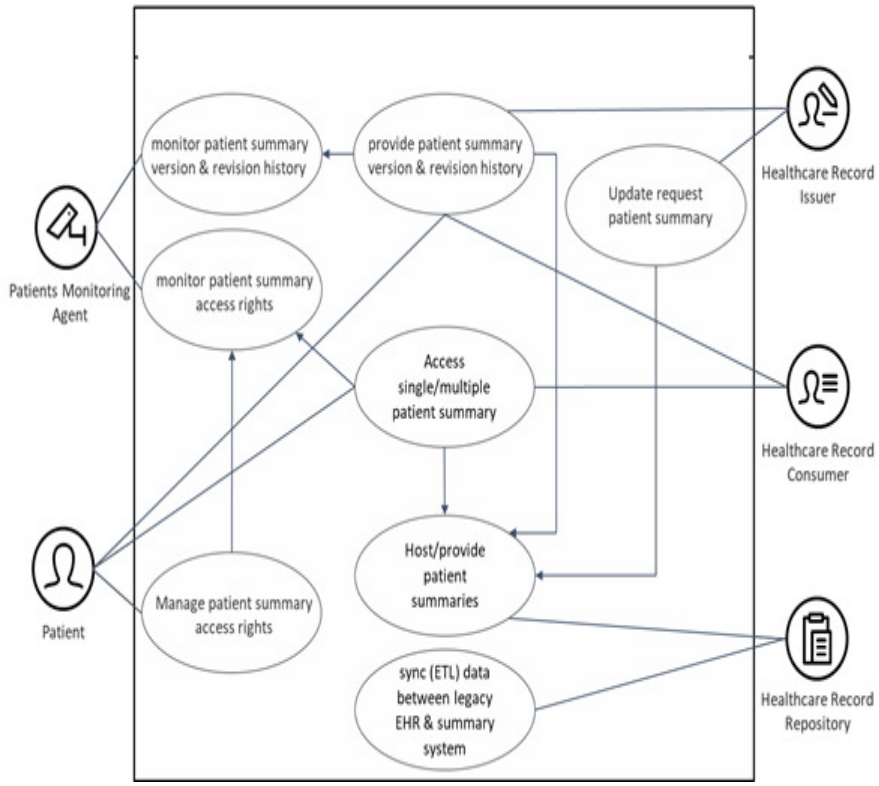
implementation for access logs and smart contracts, IPFS for storing encrypted medical files, and MongoDB for managing metadata and user roles [4]. Patients upload, share, and revoke access to their health records, while doctors view only those data that have been explicitly shared with them [5]. All interactions are immutably logged; thus, they are always traceable. The Flask-based application interface is secure and role-based, making it ready for installation at actual clinics, hospitals, and telemedicine platforms [3].

2 Existing System

Conventional EHRs function on centralized cloud systems, exposing them to threats of a single point of failure, tampering, and ingress [1]. They mostly do not have patient-centric controls, making it difficult for the patient to know who accessed their data and for what purpose. Static access control pre-established by healthcare providers itself poses an ethical dilemma and potential for loss of autonomy from the patient. Another thorny issue is unsafe sharing of data across providers due to inconsistent standards and misaligned interoperability [2].

3 Proposed System

A blockchain-based CHR promises to leverage its decentralized and secure nature to build a highly distributed software platform for storing and managing medical records. The system's acting entity is the patient with full power over his/her data. Records are encrypted and pushed onto IPFS, whereas access logs and metadata are stored in an Ethereum blockchain [3]. The access control logic is followed by smart contracts so that record reading is limited to sanctioned parties, e.g., a pre-authorized doctor [4]. One can also lift access grants at any time. All these acts shall be recorded in a manner that cannot be altered while serving the purpose of an audit. This approach... thus exploits the security and transparency that blockchain offers for patient empowerment and high interoperability between health providers [5].



4 Implementation

Implementation of the proposed system follows a well-defined sequence of steps that combine decentralized technologies with secure web practices. This section describes all significant parts of the implementation, together with their objective and interaction with other modules.

4.1 Development of the Front End Using Flask

Using the Flask web framework, the core back-end and RESTful API services were built. It enables users to be registered, to be logged-in, and to interact with the system via a clean and easy-to-use interface. Flask also manages routes and server-side logic for role-based access control. Patients, doctors, and administrators have access to the system based on their pre-defined roles to ensure data protection and features accessibility hence varied for each user. JWT (JSON Web Tokens) were used to implement secure user sessions and token-based authentication for securing sensitive routes [5].

4.2 Secure Data Management with MongoDB

For application-level data management, the MongoDB was used as a NoSQL primary database. It stores credentials of users (hashed form), and access control metadata, and mappings of uploaded file content identifiers (CIDs) generated by IPFS. The database was designed with scalability and fast look-ups in mind and integrates with Flask to validate and update user permissions in real-time. The light schema will allow for flexible extension of metadata attributes in a future upgrade [5].

4.3 Decentralize File Storage Using IPFS

To surpass the drawbacks of centralized file storage, the IPFS (InterPlanetary File System) was incorporated into the system. Medical files uploaded by patients such as prescriptions or lab reports are encrypted and stored in the IPFS network. After successful uploading, IPFS returns a unique hash, called a Content Identifier (CID), which is then stored in MongoDB and registered on the blockchain. Therefore, this decentralized approach maintains pledge confidentiality and availability of medical records without cluttering the blockchain with large files [4].

4.4 Writing Solidity-Based Smart Contracts

Smart contracts were written in Solidity and deployed onto the Ethereum blockchain. And these contracts form the access control system of the framework. The major functions include grantAccess(), revokeAccess(), and getAccessLogs(), each being triggered from an action performed by a patient from the Web interface. Smart contracts enforce that users unauthorized to make changes to the permissions cannot do so, and each change is cryptographically signed and timestamped. Execution of smart contracts brings transparency and immutability to access control, which is imperative to ethical handling and secure handling of health data [2][3].

4.5 MetaMask and Web3 Integration

MetaMask was plugged in for secure user authentication through Ethereum wallets. Somehow, the transaction on the blockchain identifies an Ethereum wallet address of a user and links it. Users dynamically authorize Web3.js frontend communication with smart contracts on the Ethereum network as well as authorize access to actions. This combination of Flask (backend) and Web3.js (frontend) with a blockchain layer of smart contracts is structured so as to allow for a decentralized-and-easy-health-record workflow [2].

4.6 Blockchain-Based Audit Logging

The system records all activities on the Ethereum blockchain. Upload of records, granting of access rights, and viewing of data are all being tracked. Logs contain

user`s wallet addresses, dates on which they happened, file references, and actions taken. This kind of audit trail using blockchain cannot be altered or erased. In this regard, the system actually instills trust and subjects all activities in line with health records to scrutiny, converting the system into an open and traceable entity [3][4].

4.7 System Integration and Security Features

The system architecture ensures modular integration of Flask, MongoDB, IPFS, and Ethereum. All API routes are secured with HTTPS, and sensitive operations employ hashed inputs and digital signatures. User data is never stored in plaintext form; file accesses are strictly controlled through smart contract permissions. The application can also be scaled and is fit for deployment on either cloud platforms or Ethereum test networks, with pot.

5 Result and Discussion

In the implementation of a blockchain-based Cloud Health Record (CHR) system, numerous developments were realized in secure handling and management of electronic health records. The integration uses Ethereum smart contracts for immutable access control, IPFS for decentralized storage of records and MongoDB for managing metadata and access logs. User testing showed that patients could easily upload and manage their own medical records with doctors given access to information only upon patient's explicit consent. This buttresses a strong patient-centric model of data ownership and fine-grained access control.

Performance benchmarking showed that all transactions, be it record uploading or granting or revocation of access, were securely logged on the blockchain with negligible latency. Data integrity was enforced through hash verification such that medical files in IPFS were not tampered with in any way. And to enhance transparency and ease of use, patients and health providers benefited from the real-time activity logging, as well as the fast web UI developed in Flask.

Security evaluations once more endorsed the framework. No unauthorized attempt was ever detected; any attempt to illicitly access data was denied by the smart contract's logic; and revocation of permissions worked in real time to enforce privacy regulations such as GDPR.

The new-age CHR, Blockchain Technology-Based Patient Data Management System, managed to combine MongoDB, IPFS, and Blockchain to achieve patient data security. For instance, the record for patient id PAT12345 in fig 5.1 implies with hashing and prev fields forming a cryptographic chain to guarantee tamper resistance on some critical health data. Any change in a block with will just invalidate the whole chain and provide integrity of data. MongoDB holds the structured data, IPFS holds the files after encryption, and the blockchain only records these access events. This, which, in turn, offers a secure party-controlled, transparent health record.

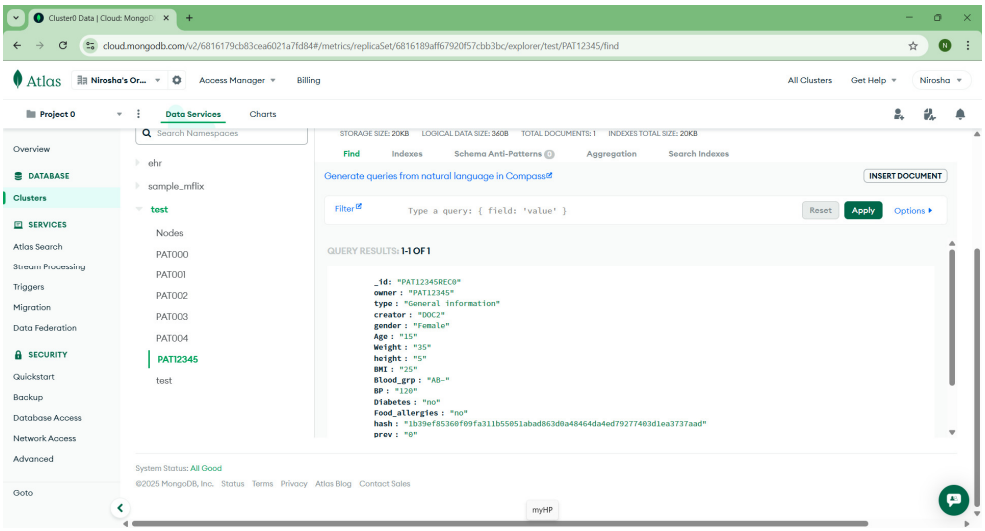


Fig 5.1 MongoDB Atlas – Backend Data Connection Between Blockchain and IPFS

The system is also QR code-based for access, where authorized users can quickly scan the unique QR code attached to the patient's account to pull up his/her health records. This ease information sharing during emergency or clinical situations providing secured instant access with no manual search. The QR code, along with blockchain permission, makes sure that only verified entities will access and see sensitive health information, providing convenience coupled with strong data privacy.

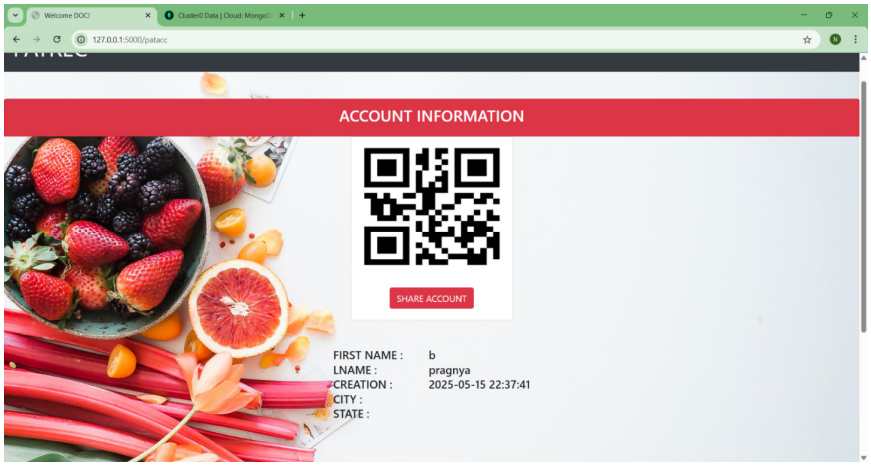


Fig 5.2 MongoDB Query Result with QR Code for Patient Health Record Access

5 Conclusion and future directions

In summary, this blockchain-implemented Cloud Health Record (CHR) System presents the right solution to secure and privately handle the Lotusor patient data in a decentralized patient-centric manner. A unique feature of the implementation was the ability of the system to store data in MongoDB, utilize IPFS for decentralized file management systems, and utilize blockchain for immutable access control so as to ensure data integrity, with privacy and traceability. Records will be cryptographically linked, time-limited access can be allowed through QR codes, and permission granting can be done online by the patient. This will create empowerment and will promote simple sharing of data between medical specialists. In future work, the system can even further be developed with AI-enabled analytics for health, mobile application support, and interoperation with national health databases for big deployments. While other encryption schemes and emergency access will of course enhance its possibilities for real-world application in high-risk scenarios, thus making it a scalable and future-proofed digital health infrastructure.

6 References

[1] Zheng, Zibin, et al. "Blockchain challenges and opportunities: A survey." *International journal of web and grid services* 14.4 (2018): 352-375.

[2] Azaria, Asaph, et al. "Medrec: Using blockchain for medical data access and permission management." *2016 2nd international conference on open and big data (OBD)*. IEEE, 2016.

[3] Xia, Qi, et al. "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments." *Information* 8.2 (2017): 44.

[4] Li, H., Zhu, L., Shen, M., Gao, F., Tao, X., & Liu, S. (2018). Blockchain-based data preservation system for medical data. *Journal of medical systems*, *42*, 1-13.

[5] Liu, Jingwei, et al. "Blockchain-aided privacy-preserving medical data sharing scheme for e-healthcare system." *IEEE Internet of Things Journal* 10.24 (2023): 21377-21388.

[6] Hurlburt, George F., and Irena Bojanova. "Bitcoin: Benefit or curse?." *It Professional* 16.3 (2014): 10-15.

[7] Singh, Sachchidanand, and Nirmala Singh. "Blockchain: Future of financial and cyber security." In *2016 2nd international conference on contemporary computing and informatics (IC3I)*, pp. 463-467. IEEE, 2016.

[8] Mermer, Gültekin Berahan, Engin Zeydan, and Suayb Sb Arslan. "An overview of blockchain technologies: principles, opportunities and challenges." *2018 26th signal processing and communications applications conference (SIU)*. IEEE, 2018.

[9] Cheng, J. C., Lee, N. Y., Chi, C., & Chen, Y. H. (2018, April). Blockchain and smart contract for digital certificate. In *2018 IEEE international conference on applied system invention (ICASI)* (pp. 1046-1051). IEEE.

[10] Bragagnolo, S., Rocha, H., Denker, M., & Ducasse, S. (2018, March). SmartInspect: solidity smart contract inspector. In *2018 International workshop on blockchain oriented software engineering (IWBOSE)* (pp. 9-18). Ieee.

[11] Steffinga, J., Lyons, L. and Bachmann, A., 2017. The Blockchain (R) evolution–The Swiss Perspective [White paper].