International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Enchancing Health Records Security Through Blockchain Protocols

Mrs. S. Francis Shamili M.E.,[1], Pavithran M[2], Pradeep M[2], Pragathish P[2], Prakash Raj M[2]

1. Department of CSE Asst Professor, Dhanalakshmi Srinivasan Engineering College, Perambalur.

2. Final Year CSE, Dhanalakshmi Srinivasan Engineering College, Perambalur.

Abstract: The traditional health record sharing system faces challenges in security, privacy, and efficient sharing. "Sec-Health" protocol, a blockchain-based solution, addresses these issues by integrating advanced cryptographic techniques. Its structured workflow includes setup, storage, sharing, and emergency access phases, ensuring controlled access and data integrity. Through blockchain and IPFS networks, users register securely in the setup phase. Health records are encrypted and stored in the blockchain network during storage. Access in the sharing phase is controlled by cryptographic material, allowing only authorized users. The emergency access phase ensures immediate and legitimate access during critical situations. Patients have dynamic control over their records through access revocation. Overall, Sec-Health offers a dynamic solution that enhances security, privacy, and collaboration in healthcare data management.

Keywords: Blockchain, Healthcare, Records, Security

I. INTRODUCTION

The healthcare sector faces significant challenges in securing patient health records, leaving sensitive information vulnerable to breaches and tampering. In response, the Sec-Health project integrates blockchain and advanced encryption to establish a secure, patient-centric data management protocol. This initiative prioritizes patient privacy, enables dynamic access control, ensures rapid emergency responses, and fosters secure collaboration for research. By leveraging consortium blockchain, governed by a national authority, Sec-Health aims to redefine healthcare data security standards. Blockchain's decentralized and tamper-proof nature offers unprecedented transparency and integrity in storing transaction records. Through its innovative approach, Sec-Health emerges as a transformative initiative poised to address critical gaps in healthcare data management and safeguard patient information in the digital age. In addition to addressing security and privacy concerns, the integration of blockchain technology in healthcare data management offers several other benefits. Blockchain enables secure and efficient interoperability among disparate healthcare systems and stakeholders, facilitating seamless exchange of patient information while maintaining data integrity. By providing a tamper-proof audit trail of transactions, blockchain enhances accountability and transparency in healthcare operations, reducing the risk of fraud and errors.

Moreover, blockchain-based solutions empower patients with greater control over their health data, enabling them to securely share information with healthcare providers, researchers, and other authorized entities. This patient-centric approach not only improves care coordination and decision-making but also enhances patient engagement and satisfaction.

II. BLOCKCHAIN

Blockchain serves as an ultra-modern digital ledger which can be tweaked to not only record monetary transactions but virtually, anything of value. The digital data that is put away on a Blockchain exists as a mutually shared— and a perpetually database. This decentralized system and its utilization has valuable benefits for virtually every industry where it is applied. Records to be stored on a Blockchain are appended to the chain only once their integrity is verified. These records are decentralized having no central storage location for a hacker to exploit. The data at any particular instance of time is hosted on millions of computers across the globe, each having the same copy that is visible to everyone present on that network.

Decentralized Storage: Blockchain serves as a decentralized ledger where health records are stored securely across a network of nodes.

Immutable Record-keeping: Once recorded on the blockchain, health records are immutable, meaning they cannot be altered or deleted. Each transaction, such as the creation or modification of a health record, is

cryptographically sealed into a block and added to the chain in chronological order.

Enhanced Security: Blockchain employs advanced cryptographic techniques to secure health records, providing robust protection against unauthorized access and breaches.

Smart Contracts for Automated Processes: Smart contracts, self-executing agreements with predefined rules, automate various processes within the Sec-Health protocol.

Interoperability and Collaboration: Blockchain facilitates interoperability by enabling seamless sharing of health records among different healthcare providers and systems. This interoperability promotes collaboration and information exchange, leading to improved patient care and outcomes.

III. BLOCKCHAIN ARCHITECTURE

The architecture for blockchain technology in the context of the Sec-Health project involves several key components and layers designed to ensure secure and efficient healthcare data management. Here's a high-level overview of the architecture:

A. Network Layer:

Nodes: The network consists of multiple nodes, which can be distributed across various geographical locations. Nodes are individual computers or servers that participate in the blockchain network.

Peer-to-Peer Communication: Nodes communicate with each other using a peer-to-peer (P2P) network protocol. This enables the exchange of data, transactions, and blocks among network participants.

B. Blockchain Layer:

Blocks: Blocks are containers that store a batch of valid transactions. Each block contains a cryptographic hash of the previous block, creating a chain of blocks (hence the term "blockchain").

Transactions: Transactions represent the exchange of data or assets between network participants. In the context of Sec-Health, transactions include the creation, access, and sharing of healthcare records.

By integrating these components and layers, the blockchain architecture for the Sec-Health project establishes a secure, transparent, and interoperable platform for healthcare data management, ensuring the privacy, security, and integrity of patient health records.

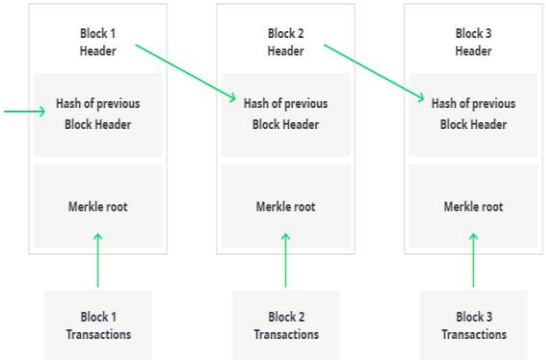

Figure 1: Sequence of Blocks in a Blockchain

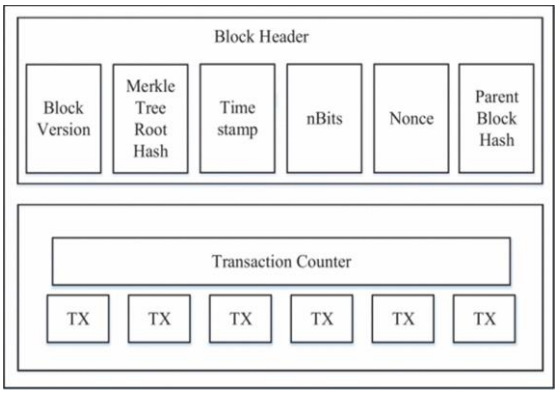

Figure 2: Structure of a single block

Each block consists of the block header and the block body as shown in Figure 2. A block header contains following information:

The block body is composed of a transaction counter and transactions. Maximum number of transactions that a block can contain depends on the block size and the size of each transaction

1. Block version: specifies block validation rules to be followed.
2. Merkle tree root hash: the hash value of all the transactions in the block.[15]
3. Timestamp: current time as seconds.

4. nBits: target threshold of a valid block hash.
5. Nonce: a 4-byte field, which usually starts with 0 and increases for every hash calculation [15]
6. Parent block hash: a 256-bit hash value that points to the previous block.

Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions

IV. BLOCKCHAIN SECURITY

Blockchain technology offers several inherent security advantages, which make it an attractive solution for various applications, including healthcare data management like the Sec-Health project.

A. Decentralization:

Blockchain operates on a decentralized network of nodes, eliminating the need for a central authority. This decentralization makes it inherently resistant to single points of failure and reduces the risk of data manipulation or tampering.

B. Immutable Ledger:

Once data is recorded on the blockchain, it cannot be altered or deleted. Each block contains a cryptographic hash of the previous block, creating a chain of blocks that is virtually tamper-proof. This immutability ensures the integrity and transparency of transactions.

C. Encryption:

Blockchain employs advanced cryptographic techniques to secure data and transactions. Transactions are encrypted using public-key cryptography, ensuring that only authorized parties can access and decrypt sensitive information.

D. Reduced Cybersecurity Risks:

By decentralizing data storage and distribution, blockchain reduces the risk of cyber attacks such as DDoS (Distributed Denial of Service) attacks, data breaches, and unauthorized access. The distributed nature of blockchain networks makes them less susceptible to hacking and cyber threats compared to centralized systems.

V. EXISTING METHODOLOGY

Electronic Health Records (EHRs), such as patient's medical history, are one of the most widely employed resources, providing a wide view of a patient's medical status. EHRs are commonly originated and shared with collaborators (e.g., physicians, nurses) through cloud computing systems, which results in a more convenient approach to managing such records. Only authorized collaborators should access health records (confidentiality and access control properties). Records must also be protected from unauthorized modifications (integrity property). Mechanisms must also exist to legitimately grant access to records in emergency situations (emergency access property), and to anonymized records for research purposes (anonymity property). Besides, the properties of access revocation and interoperability must also be addressed. Those properties motivate the design of solutions to secure healthcare information systems. A number of literature proposals provide schemes based on centralized servers to store and share health records. The security of such solutions rely on the fact that the server is trusted not to disclose sensitive data, such as information related to user credentials and patient records. This result in a single point that, when compromised, can make the entire system fail. Recent approaches use of decentralized approaches to secure health records. For instance, blockchain, a technology that improves data security by allowing online data transactions in a decentralized fashion, has been adopted in different protocols. Although these schemes do not present a single point of failure, they still lack an integrated approach that covers all of the aforementioned health records properties, then presenting security limitations.

VI. PROPOSED METHODOLOGY

In proposed system, implement a blockchain-based protocol called Sec-Health, which enhances the schemes employed in the previous protocol to fulfill

the security properties of confidentiality, access control, and integrity. Sec-Health includes novel schemes to address additional properties, i.e., emergency access, access revocation, anonymity, and interoperability. An authority is responsible for managing user's registration and attesting that cryptographic material is valid, while a blockchain and an IPFS network store data related to health records. Several participants are considered the system users, as follows. A collaborator (e.g., physician, nurse) generates health records for patients and accesses, under patient consent, records generated by other collaborators. Research entities access anonymized health records to conduct researches. Attendants are call center professionals who handle initial steps of emergency sessions according to required information received from a phone caller. Finally, emergency servers are participants that assist collaborators to legitimately gain access to health records in emergency sessions. Every health record is encrypted with a AES with access policy elaborated by

the patient. Therefore, an attacker attempting to maliciously access a record in our scheme would need to corrupt the majority of the servers in order to obtain a sufficient number of decryption parts. The set of four phases is composed of setup, storage, sharing, and emergency access. They include mechanisms that satisfy four health records properties, namely confidentiality, access control, integrity, and emergency access.

The protocol begins with the setup phase, in which blockchain and IPFS networks are created, and users are registered in the system. The authority attests all the public data (e.g., participants' public key) necessary to run the system, which are stored in the blockchain. In the storage phase, a collaborator generates a health record for a patient, who stores it in the IPFS network and its metadata in the blockchain in a secure fashion such that another collaborator can later access the record. After this, the designated collaborator can access the health record, in the sharing phase, if they own the required cryptographic material for this purpose. The emergency access phase occurs when a patient needs emergency medical care and has no physical conditions (e.g., may be unconscious) to give available collaborators access permission to her health record. This phase runs in a collaborative way (between the emergency servers, collaborators and call center attendant) such that the patient can later verify who participated in the emergency session and had access to her health record. After granting access to a health record for a collaborator, the patient can revoke this access right whenever she wants by means of the access revocation mechanism in an interaction with the blockchain network. With the anonymity mechanism, a collaborator can provide a health record for research studies under patient consent.

VII. SYSTEM ARCHITECTURE

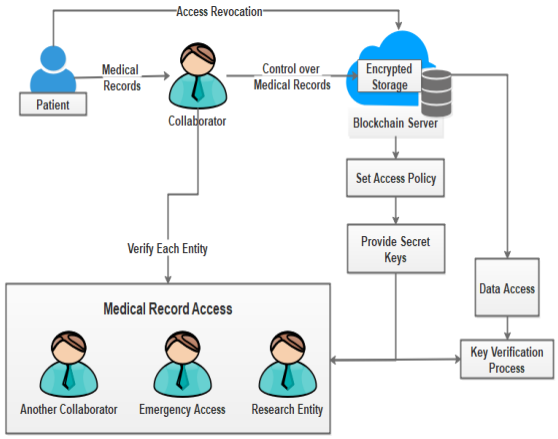

Figure 3: System Architecture

VIII. RELATED WORKS

Ganiga et.al,…[1] The proposed security framework for Electronic Health Record (EHR) systems addresses the critical aspects of integrity, availability, and confidentiality of health records. By leveraging tools such as STRIDE modeling and DREAD risk assessment, the framework identifies and mitigates threats posed to the EHR system. Various attacks and vulnerabilities are analyzed, and appropriate countermeasures are discussed to protect health information stored in the cloud-based EHR database. This framework provides structured security processes for healthcare application developers, enabling them to evaluate security threats and implement suitable countermeasures. It incorporates security rules encompassing administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of the EHR system. Recognizing the significance of real-time patient data and population health management, the framework facilitates seamless connectivity across all levels of the public health system, regardless of geographical boundaries. However, it acknowledges that the client component of the EHR system is particularly vulnerable to attacks due to its role in viewing, entering, and modifying health information. Similarly, compromising the server grants attackers complete control over the system, leading to potential exposure, alteration, or destruction of health information. Network compromises pose additional risks such as eavesdropping and data alteration during transit.

Masud et.al,…[2] The proposed scheme for cloud-based E-healthcare services offers a robust and lightweight solution to address potential threats and ensure secure access for stakeholders. By leveraging a key derivation function (KDF), the scheme generates multiple keys for end-to-end encryption, enhancing data security and preventing unauthorized access. Access to cloud services is granted based on stakeholder identity and association, ensuring privacy and confidentiality of medical records. In the hospital environment, where staff face challenges in handling and storing patient records, the proposed scheme alleviates manual tasks by storing medical records in the cloud. The scheme distinguishes between user devices, gateways, and cloud entities. All entities execute identical cryptography functions, ensuring consistency and security throughout the system. Key Derivation Function (KDF) plays a crucial role in deriving secret keys from the master key, enhancing encryption strength and protecting sensitive information.

Kumar et.al,…[3] The state-of-the-art cloud-centric IoMT-enabled smart healthcare system with public verifiability leverages an escrow-free identity-based aggregate signcryption (EF-IDASC) scheme to ensure secure and efficient data transmission. This novel system fetches medical data from various sensors implanted on the patient's body, signcrypts, and aggregates them using the EF-IDASC scheme. Subsequently, the data is outsourced to a medical cloud server via a smartphone, safeguarding the patient's identity and medical information. In this system, data is signcrypted by the Body Monitoring System (BMS) using its private key, which can only be decrypted using the private key of the Smart Device (SD) and BMS's identity. Unauthorized interception of the original data is prevented as it requires the private key of SD/BMS, which is derived from the Network Manager's (NM) master key and Key Production System's (KPSs) secret keys. Registration in this system involves authentication and registration by NM, followed by the issuance of a private key to each entity. Communication between entities is only permitted if they were previously registered with NM.

Abunadi et.al,…[4] Proposes a blockchain security framework (BSF) to effectively and securely store and keep EHRs. It presents a safe and proficient means of acquiring medical information for doctors, patients and insurance agents while protecting the patient's data. Electronic health records (EHR) are regulated by health centers instead of patients, making it difficult to obtain medical advice from various health centers. Thus, patients need to concentrate on restoring the management of their health details and their medical information. The quick evolution of blockchain technology encourages population healthcare, including access to patient information and medical data. In the BSF-EHR system, the miner node is the EHR system server and both the doctor and patient are full nodes. The insurance agent plays the role of the light nodes. In the BSF-EHR system, a large number of doctors and patients and also insurance agents are available. Therefore, access control is necessary. Our BSF-EHR system provides access control.

Zhuang et.al,…[5] Developed a blockchain model to protect data security and patients' privacy, ensure data provenance, and provide patients full control of their health records. By personalizing data segmentation and an "allowed list" for clinicians to access their data, this design achieves patient-centric HIE. To utilize the unique technological capabilities of blockchain for patient centric HIE, we have implemented a private Ethereum blockchain system with multiple smart-contract. A system administrator from each healthcare facility will create a touchpoint for each patient's visit after the EHR is ready and input the related primary information into a smart contract for future indexing. Clinicians can select records through the touchpoints after being granted access to the patient's records without identifying the hospitals storing those records. The subsequent exchange of data among the involved remote healthcare facilities will include data encryption and use of the blockchain system to send and retrieve decryption keys.

IX. CONCLUSION

The Sec-Health protocol presents a comprehensive and innovative solution to the multifaceted challenges inherent in healthcare data management. By leveraging blockchain technology, advanced encryption, and decentralized storage, Sec-Health ensures the utmost security, privacy, and interoperability of health records. The modular design encompasses key functionalities, including secure framework creation, encrypted health record storage, patient-controlled access privileges, robust blockchain infrastructure, collaborator access mechanisms, emergency access procedures, research entity interactions, and dynamic access revocation. Patient-controlled access privileges empower individuals to define who can access their health records, adding a layer of dynamic control and transparency. Collaborators benefit from secure access mechanisms, while emergency situations are addressed with a swift and legitimate emergency access module. Research entities can conduct studies using anonymized health records, fostering collaboration between healthcare practitioners and researchers. The access revocation module gives patients the dynamic control to revoke access rights, emphasizing patient-centric data management.

X. REFERENCES

[1] Ganiga, Raghavendra, Radhika M. Pai, and Rajesh Kumar Sinha. "Security framework for cloud based electronic health record (EHR) system." International Journal of Electrical and Computer Engineering 10, no. 1 (2020): 455.

[2] Masud, Mehedi, Gurjot Singh Gaba, Karanjeet Choudhary, Roobaea Alroobaea, and M. Shamim Hossain. "A robust and lightweight secure access scheme for cloud based E-healthcare services." Peer-to-peer Networking and Applications 14, no. 5 (2021): 3043-3057.

[3] Kumar, Mahender, and Satish Chand. "A secure and efficient cloud-centric internet-of-medical-things-enabled smart healthcare system with public verifiability." IEEE Internet of Things Journal 7, no. 10 (2020): 10650-10659.

[4] Abunadi, Ibrahim, and Ramasamy Lakshmana Kumar. "BSF-EHR: blockchain security framework for electronic health records of patients." Sensors 21, no. 8 (2021): 2865.

[5] Zhuang, Yan, Lincoln R. Sheets, Yin-Wu Chen, Zon-Yin Shae, Jeffrey JP Tsai, and Chi-Ren Shyu. "A patient-centric health information exchange framework using blockchain technology." IEEE journal of biomedical and health informatics 24, no. 8 (2020): 2169-2176.

[6] Zghaibeh, Manaf, Umer Farooq, Najam Ul Hasan, and Imran Baig. "Shealth: A blockchain-based health system with smart contracts capabilities." IEEE Access 8 (2020): 70030-70043.

[7] T. de Oliveira, Marcela, Alexandros Bakas, Eugene Frimpong, Adrien ED Groot, Henk A. Marquering, Antonis Michalas, and Silvia D. Olabarriaga. "A break-glass protocol based on ciphertext-policy attribute-based encryption to access medical records in the cloud." Annals of Telecommunications 75 (2020): 103-119.

[8] Xu, Yang, Cheng Zhang, Guojun Wang, Zheng Qin, and Quanrun Zeng. "A blockchain-enabled deduplicatable data auditing mechanism for network storage services." IEEE Transactions on Emerging Topics in Computing 9, no. 3 (2020): 1421-1432.

[9] Li, Jiaxing, Jigang Wu, Guiyuan Jiang, and Thambipillai Srikanthan. "Blockchain-based public auditing for big data in cloud storage." Information Processing & Management 57, no. 6 (2020): 102382.

[10] Rajput, Ahmed Raza, Qianmu Li, and Milad Taleby Ahvanooey. "A blockchain-based secret-data sharing framework for personal health records in emergency condition." In Healthcare, vol. 9, no. 2, p. 206. MDPI, 2021.