'National Conference on Recent Advances of Computational Intelligence Techniques in Science, Engineering and Technology'
International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Preserving Privacy in EHR Sharing with Consortium Blockchain and Searchable Encryption

Heena Kousar*, Ammu Bhuvana S, Madhushree, Khallikkunaisa
Department of Computer Science & Engineering, VTU/EPCET/Bengaluru, Karnataka, India

ABSTRACT
This research paper presents an innovative protocol that utilizes blockchain technology to facilitate secure and privacy-preserving sharing of Electronic Health Records (EHRs). By harnessing the decentralized, anonymous, and verifiable nature of blockchain, the protocol effectively tackles the data security and privacy concerns commonly associated with cloud-based EHR sharing systems. The protocol offers data requesters the capability to search for relevant EHRs on the EHR consortium blockchain using specific keywords. With explicit authorization from the data owner, the requesters can retrieve re-encryption ciphertext from the cloud server. To ensure robust data security, privacy preservation, and access control, the protocol incorporates searchable encryption and conditional proxy re-encryption techniques. To guarantee system availability, a proof of authorization mechanism is implemented as the consensus mechanism for the consortium blockchain. This mechanism rigorously verifies and validates the authorization of data requesters, thus enhancing the overall security and integrity of the system.
Keywords: Datasharing, Electronic Health Records, Privacy preservation, Blockchain

I. INTRODUCTION

EHR sharing has attracted significant attention and research from industry and academia, particularly in the areas of privacy preservation, data security and interoperability [2]. Privacy preservation is crucial as EHRs contain personal and highly sensitive information that must be protected to safeguard patients reputation and well-being. Similarly, data security is essential to ensure that only authentic information is included in EHRs, as forged or modified data can undermine the effective utilization of these records. Lastly, interoperability plays a vital role in allowing patients to have control over the access rights of their EHRs and facilitating the seamless exchange of records between different healthcare institutions.

A HER sharing protocol based on a consortium blockchain is proposed which ensures secure and privacy-preserving data access. Only authorized data requesters who possess the search trapdoor can obtain relevant keywords and information. The blockchain accounts handle authorization and other access services, guaranteeing privacy protection. Additionally, the cloud re-encrypts the EHR ciphertext and securely shares it with the agreed-upon data requester.

In this paper, we first provide an overview of related research in Section II, Section III presents the key technologies necessary for our protocol. Section IV discusses the system architecture, EHR consortium blockchain, threat model and security goals. It is then delve into the protocol details and security proof in Section V. Atlast summarize the paper and discuss the future implementation.

II. RELATEDWORK

In this section, we discuss works that focus on EHR sharing with the help of cloud technology and blockchain technology

A. EHR SHARING WITH CLOUD

Access control schemes and searchability and interoperability of EHR sharing have been improved using cloud technology and blockchain technology. To ensure data security during the process of EHR sharing, access control schemes based on the cloud have been introduced [3]-[5]. A study proposed a new method called ciphertext-policy attribute-based sign-encryption and secure sharing of personal health records in cloud computing, which enables fine-grained access control. Another study [4] proposed an efficient and secure fine-grained access control scheme for authorized users to access EHRs in cloud storage. Furthermore, [5] developed a hierarchical comparison-based encryption scheme and a dynamic policy updating scheme using the proxy-encryption technique to achieve dynamic access control in cloud-based EHR systems.To enhance the searchability and interoperability of EHR [6] sharing, a study presented a cloud-based EHR system that supports fuzzy keyword search, ensuring secure data sharing and effective utilization of the EHRs. Another study utilized conjunctive keyword search with proxy re-encryption to create a secure EHR search scheme for data sharing between different medical institutions. Moreover, proposed a general framework for secure sharing of EHRs, allowing patients to securely store and share their EHRs on a cloud server, while enabling doctors to access the EHRs in the cloud. In addition, a study proposed a blockchain-based secure and privacy-preserving EHR sharing protocol, which allows data requester to search desired keyword from EHRs without revealing the content of the EHRs. The protocol ensures data security and privacy preservation via consortium blockchain.

B. EHR SHARING WITH BLOCKCHAIN

Data Security: Blockchain technology can enhance the security of electronic health records (EHRs) by providing a tamper-resistant and immutable ledger. Each transaction or modification made to the EHR is recorded as a block, linked to previous blocks, and distributed across a network of computers. This decentralized nature makes it difficult for malicious actors to alter or manipulate the data without consensus from the network [10]. Interoperability: Blockchain has the potential to improve interoperability between different healthcare systems. Since blockchain operates on a distributed ledger, it can facilitate seamless data exchange and integration among various healthcare providers, regardless of their underlying EHR systems. This can help eliminate data silos and improve care coordination.

Data Integrity: Blockchain's immutability ensures the integrity of EHRs. Once data is recorded on the blockchain, it becomes virtually impossible to modify or delete it without leaving a trace. This feature can help address issues related to data tampering and ensure the accuracy and reliability of patient health records.The

architecture mentioned, which combines blockchain technology with intelligent contracts and user-generated acceptable policies, can be a promising approach to enhancing the security control of personal data in health information exchange. By leveraging blockchain's decentralized and immutable nature, along with smart contracts' automation capabilities, it is possible to create a robust framework for data security [11]. The conceptual design you mentioned, which combines blockchain technology with cloud storage, aims to facilitate safe and transparent sharing of personal continuous-dynamic health data. Here's a high-level overview of this design:

Blockchain Network: The design utilizes a blockchain network as a decentralized and immutable ledger. Health data is encrypted and stored on the blockchain, ensuring its integrity and protection from unauthorized access. The blockchain's transparency allows for auditing and traceability of data transactions.

Cloud Storage: In addition to the blockchain, the design incorporates cloud storage for efficient and scalable data storage. While the blockchain stores metadata and references to health data, the actual data itself is securely stored in the cloud. Cloud storage enables the storage of large volumes of continuous and dynamic health data.

Secure Data Sharing: Users can securely share their personal health data through the blockchain network. The blockchain facilitates the creation of secure and transparent transactions when sharing data. Users can define access permissions and consent requirements using smart contracts, ensuring that data is shared only with authorized parties and with the necessary consent.

III. PRELIMINARIES

The technical preliminaries mentioned in this section pertain to the concepts of bilinear maps and complexity assumptions. Here's a breakdown of the key definitions and properties:

Bilinear Maps:

Bilinear Map (e^): A bilinear map is denoted as e^ and operates between two cyclic groups of the same prime order. It takes two elements from the first group (F1) and maps them to an element in the second group (F2).

Admissible Bilinear Map: An admissible bilinear map, denoted as e^, satisfies the following properties: a. e^(aR, bS) = e^(R, S)^(ab) for all R, S ∈ F1 and a, b ∈ Zq* (non-zero integers modulo q). b. e^(R, S) = e^(S, R) (symmetric property). c. e^(R + S, T) = e^(R, T) * e^(S, T) for all R, S, T ∈ F1 (bilinearity property). d. There exist elements R, S ∈ F1 such that e^(R, S) ≠ 1 (mod F2). e. The bilinear map e^ can be efficiently computed.

Complexity Assumptions:

Elliptic Curve Discrete Logarithm Problem (ECDLP): In this problem, we consider an elliptic curve denoted as E. The primitive element on the curve is P, and X is another element on the elliptic curve. Given pE as the number of points on the curve, the ECDLP aims to find an integer b (1 ≤ b ≤ pE) such that P + P + ... + P = bP = X. The ECDLP is assumed to be computationally difficult, meaning that finding the value of b from the given elements is challenging and no efficient algorithm exists for solving it.

In cryptosystems, the private key is usually an integer, and the public key is a point on the curve with coordinates X (xX,*yx*).

ECDLP Assumption. It is assumed that it is difficult to solve the ECDLP in polynomial time.

Definition 2: The Decision Linear Diffie-Hellman Problem (DLDH) is defined in the context of an elliptic curve E and a cyclic group G1 of prime order Q. Let P1, P2, and P3 be random elements in G1, and let a1, a2, and a3 be random numbers in Zq*. The DLDH problem is formulated as follows:

Given the tuple (P1, P2, P3, a1P1, a2P2, a3P3) ∈ F1 as input, the goal is to determine whether a3 is equal to a1 + a2 or not. The output is 1 if a3 = a1 + a2, and 0 otherwise.

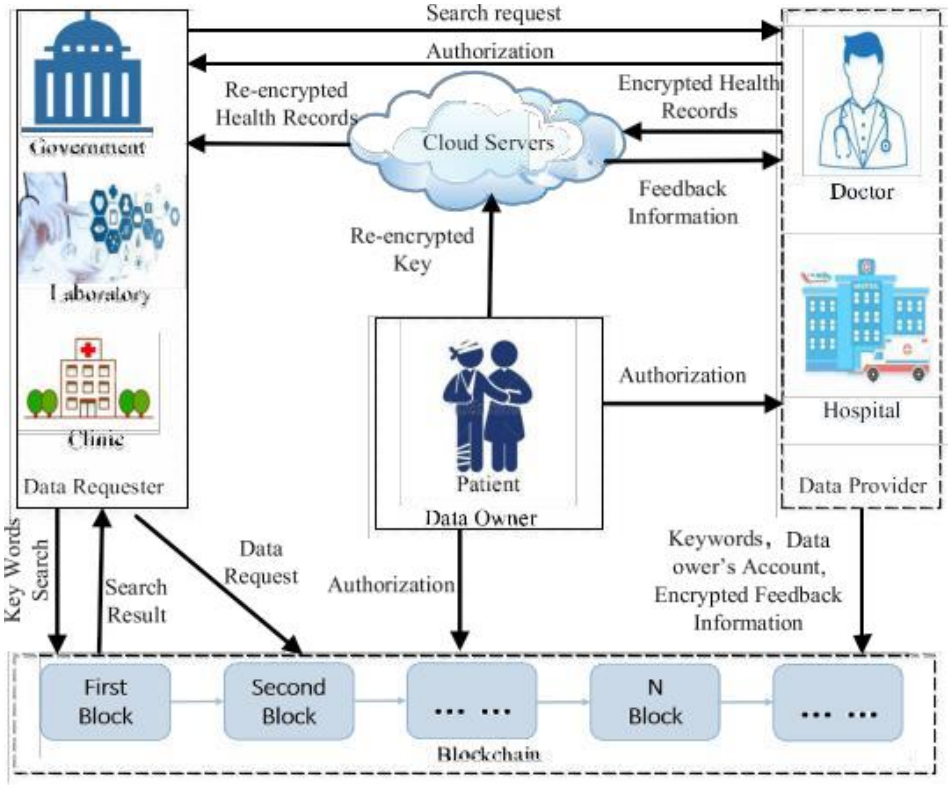
The advantage of an algorithm A in deciding the DLDH problem in F1 is defined as the probability that A correctly determines the equality a3 = a1 + a2 when given the input tuple (P1, P2, P3, a1P1, a2P2, (a1 + a2)P3). Mathematically, it is expressed as:

Pr[A(P1, P2, P3, a1P1, a2P2, (a1 + a2)P3) = 1]

The advantage of an algorithm A represents how well it can solve the DLDH problem, with a higher advantage indicating a better ability to distinguish valid solutions from invalid ones.

IV. SYSTEM ARCHITECTURE

There are five entities in the proposed framework: Data owners (DO), data providers (DP), cloud servers (CS), blockchain (BC), and data requesters (DR), as shown in Fig. 1.



- **DATAOWNERS**

In the given context, "DO" refers to data owners, who are the patients visiting doctors in hospitals or medical institutions for medical services. The data owners are the source of health records, and as such, they have ownership and control rights over their data. To facilitate data sharing, the data owners need to register an account on the EHR (Electronic Health Records) consortium blockchain.

- DATA PROVIDERS

In the given context, "DO" refers to data owners, who are the patients visiting doctors in hospitals or medical institutions for medical services. The data owners are the source of health records, and as such, they have ownership and control rights over their data. To facilitate data sharing, the data owners need to register an account on the EHR (Electronic Health Records) consortium blockchain.

If a new DP wants to join the blockchain, he or she has to take three steps:

- Register an account with the EHR consortium.•
- Submit a recommendation letter signed by one commissioner and send it to all of the•
- Get at least 2⁄3 of the authorizations from commissioners.

- CLOUD SERVER

The cloud server's primary role in the system is to securely store the encrypted Electronic Health Records (EHRs) provided by the Data Providers (DPs). It ensures that the stored files are kept confidential and intact, and it also shares the file location information with the Data Owners' (DOs) accounts on the EHR consortium blockchain. However, it's worth noting that although the cloud server operates honestly and follows the prescribed procedures, it may have a natural curiosity about the data it handles. Additionally, the cloud server is responsible for re-encrypting the EHRs using the appropriate re-encryption key when required, further safeguarding the privacy and security of the records.

- DATA REQUESTERS

Data requesters, which can include government entities, laboratories, clinics, and other relevant organizations, are key stakeholders in the proposed system for accessing patients Electronic Health Records (EHRs). Their role involves obtaining a search trapdoor from the Data Provider (DP) to search for specific keywords within the blockchain. Based on the search results, they can then send a formal request to the Data Owner (DO) for authorization to access the desired EHRs.

Once the data requesters receive authorization from the DO, they are granted access to the encrypted health records stored on the cloud server. These health records are securely maintained to ensure confidentiality and integrity. As part of their interaction with the system, the data requesters' actions generate service transactions, which are added to the transaction pool. This active involvement positions them as service transaction senders within the blockchain network.

Data requesters have the flexibility to join or exit the blockchain network at any time, functioning as regular users. They have visibility into the entire consensus process and can observe the system's operation. Additionally, they have the privilege of enjoying the services provided by the system

V. PROPOSED MODEL

The process of the proposed protocol is represented in Fig. 2.The protocol is made up of three layers: Data generation layer, data storage layer, and data sharing layer.

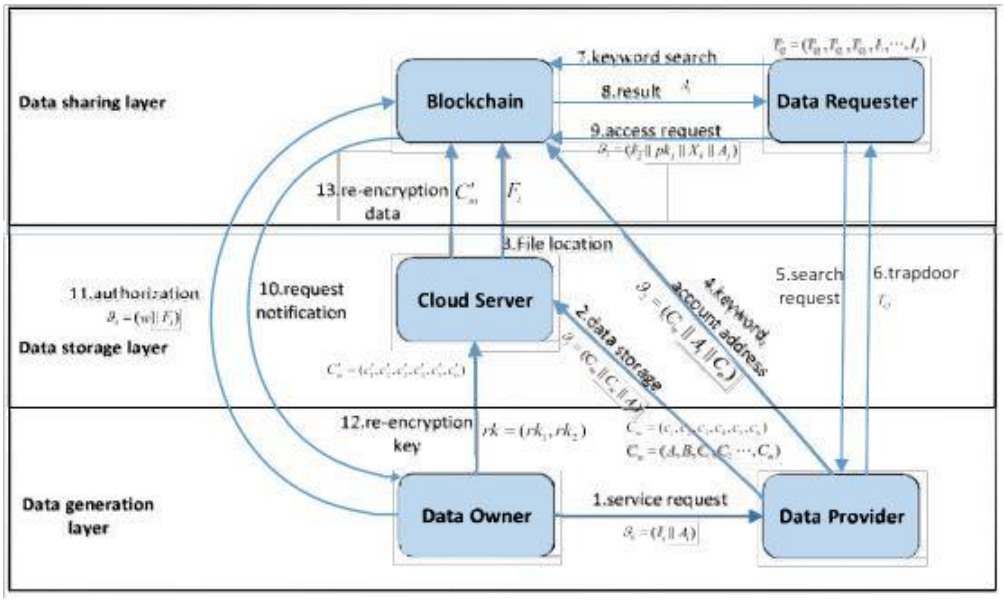


Fig 2: Proposed Protocol

When a patient, referred to as DO with identity Ii, visits a hospital for medical services, they are required to register an account in the EHR consortium blockchain. The EHR consortium blockchain generates an account address and private key, which are then sent to the patient for secure access.

The patient, denoted as i, transmits a data packet ϑ0 = (Ii || Ai) to a doctor, identified as k. The original Electronic Health Record (EHR) for patient i is generated through interactions with doctor k, who is the Data Provider (DP). The DP extracts a series of keywords from the EHR. Subsequently, the DP encrypts the EHR, denoted as m, using the patient's public key (pki), the DP's private key (xk), and the keyword wi. This encryption process produces the EHR ciphertext (Cm). Additionally, the DP encrypts the keyword wi using their own public key (Xk), resulting in the keyword ciphertext (Cw). The DP then sends the data packet ϑ1 = (Cm Cw Ai) to the cloud server for storage. Once the cloud server safely stores the data, it sends the file location (Fi) to the DO's account.

When data requesters (DRs) need to search for specific Electronic Health Records (EHRs), they begin by submitting a search request to the Data Provider (DP). If the request is approved, the DRs are provided with a trapdoor (TQ) to facilitate their search. Using this trapdoor, the DRs can explore the blockchain and locate the matched EHRs, along with the associated Data Owner's (DO) account address (Ai).

Afterwards, the DRs initiate an access request by sending a data packet ϑ3 = (Ij pkj Xk Aj) to the DO's account. Upon receiving this request, the DO responds by granting authorization. The authorization includes essential details such as the file location (Fi) and the corresponding keyword (wi). Additionally, the DO generates a re-encryption key (rk) and shares it with the Cloud Server (CS). The CS utilizes this key to perform proxy re-encryption on the required ciphertext.

Lastly, the DRs utilize their private key (skj) to decrypt the re-encrypted ciphertext (Cmr), enabling them to securely access the desired EHRs and retrieve the relevant information.

VI. CONCLUSION

In our research, we have proposed an original scheme for sharing Electronic Health Records (EHRs) using blockchain technology. Our approach focuses on ensuring data security and privacy preservation during the sharing process across diverse medical institutions. We have introduced a framework that combines cloud-assisted storage and blockchain to facilitate efficient EHR sharing between entities. The cloud serves as the storage provider for the encrypted EHR ciphertext, while the EHR indexes are stored securely on the EHR consortium blockchain. To address data security and privacy concerns, we have designed an architecture and protocol that incorporate conjunctive keyword-searchable encryption and conditional proxy re- encryption. These mechanisms enable efficient searchability of EHRs based on multiple keywords while ensuring secure data transfer between authorized parties.

For future work, our plan is to implement and optimize the proposed scheme using the Hyperledger Fabric blockchain platform. This will involve refining the smart contracts responsible for executing the data sharing algorithms, thereby enhancing the functionality and performance of our system.

should be below the figures; table heads should appear above the tables. Insert figures and tables after they are cited in the text. Use the abbreviation "Fig. 1", even at the beginning of a sentence. We suggest that you use

Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions. Authors are strongly encouraged not to call out multiple figures or tables in the conclusion these should be referenced in the body of the paper.

VII. REFERENCES

[1]. H. K. Patil and R. Seshadri, "Big data security and privacy issues in healthcare," in Proc. IEEE Int. Congr. Big Data, Anchorage, AK, USA, Jun./Jul. 2014, pp. 762–765.

[2]. J. Li and X. Li, "Privacy preserving data analysisin mental health researc," n Proc. IEEE Int. Congr. Big Data, New York, NY, USA, Jun./Jul. 2015 pp. 95–101.

[3]. J. Liu, X. Huang, and J. K. Liu, "Secure sharing of Personal Health Records in cloud computing: Ciphertext-policy attribute-based signcryption," Future Gener. Comput. Syst., vol. 52, pp. 67–76, Nov. 2015.

[4]. X. Liu, Y. Xia, W. Yang, and F. L. Yang, "Secure and effificient querying over personal health records in cloud computing," Neuro Comput., vol. 274, pp. 99–105, Jan. 2018.

[5]. X. Liu, Q. Liu, T. Peng, and J. Wu, "Dynamic access policy in cloud based personal health record (PHR) systems," Inf. Sci., vol. 379, pp. 62–81, Feb. 2017.

[6]. Z. Liu, J. Weng, J. Li, J. Yang, C. Fu, and C. F. Jia, "Cloud-based electronic health record system supporting fuzzy keyword search," Soft Comput., vol. 20, pp. 3243–3255, Aug. 2016 .

[7]. X. Wang, A. Zhang, X. Ye, and X. Xie, "Secure-aware and privacy preserving electronic health record searching in cloud environment," Int. J. Commun. syst., vol. 32, p. e3925, May 2019. doi: 10.1002/dac.3925.

[8]. M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang, "A general framework for secure sharing of personal health records in cloud system," J. Comput. Syst. Sci., vol. 90, pp. 46–62, Dec. 2017.

[9]. G. Zyskind, O. Nathan, and A. S. Pentland, 'Decentralizing privacy: Using blockchain to protect personal data," in Proc. IEEE Secur.Privacy Workshops, vol. 90, May 2015, pp. 180–184.

[10]. S. Amofa, E. B. Sifah, K. O.-B. Agyekum, S. Abla, Q. Xia, J. C. Gee, and J. B. Gao, "A blockchain-based architecture framework for secure sharing of personal health data," in Proc. IEEE 20th Int. Conf. e-Health Netw., Appl. Services (Healthcom). Ostrava, Czech Republic, 2018, pp. 1–6.

[11]. X. Zheng, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Mere, "Blockchain-based personal health data sharing system using cloud storage," in Proc. IEEE 20th Int. Conf. e-Health Netw., Appl. Services (Health com). Ostrava, Czech Republic, Sep. 2018, pp. 1–6.

[12]. T. Mikula and R. H. Jacobsen, "Identity and access management with blockchain in electronic healthcare records," in Proc. 21st Euromicro Conf. Digit. Syst. Design (DSD), Prague, Czech Republic, 2018, pp. 699–706.