GRIFFITH UNIVERSITY

Cross-chain Sharing of Personal Health Records: Heterogeneous and Interoperable Blockchains

Author

Lv, Y, Li, X, Wang, Y, Chen, K, Hou, Z, Feng, R

Published

2024

Conference Title

2024 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)

Version

Accepted Manuscript (AM)

DOI

10.1109/BIBM62325.2024.10822679

Rights statement

This work is covered by copyright. You must assume that re-use is limited to personal use and that permission from the copyright owner must be obtained for all other uses. If the document is available under a specified licence, refer to the licence for details of permitted re-use. If you believe that this work infringes copyright please make a copyright takedown request using the form at https://www.griffith.edu.au/copyright-matters.

Downloaded from

https://hdl.handle.net/10072/435600

Griffith Research Online

https://research-repository.griffith.edu.au

Cross-chain Sharing of Personal Health Records: Heterogeneous and Interoperable Blockchains

Yongyang Lv[1], Xiaohong Li[1], Yingwenbo Wang[1], Kui Chen[1], Zhe Hou[2] and Ruitao Feng[3,*]
[1]College of Intelligence and Computing, Tianjin University, Tianjin, China
[2]School of Information and Communication Technology, Griffith University, Brisbane, Australia
[3]Faculty of Science and Engineering, Southern Cross University, Gold Coast, Australia
*Corresponding author
Emails: lvyongyang@tju.edu.cn, Xiaohongli@tju.edu.cn, wangyingwenbo@tju.edu.cn,
chen_kui@tju.edu.cn, z.hou@griffith.edu.au, ruitao.feng@scu.edu.au

***Abstract*—With the widespread adoption of medical informatics, a wealth of valuable personal health records (PHR) has been generated. Concurrently, blockchain technology has enhanced the security of medical institutions. However, these institutions often function as isolated data silos, limiting the potential value of PHRs. As the demand for data sharing between hospitals on different blockchains grows, addressing the challenge of cross-chain data sharing becomes crucial. When sharing PHRs across blockchains, the limited storage and computational capabilities of medical Internet of Things (IoT) devices complicate the storage of large volumes of PHRs and the handling of complex calculations. Additionally, varying blockchain cryptosystems and the risk of internal attacks further complicate the cross-chain sharing of PHRs. This paper proposes a scheme for sharing PHRs across heterogeneous and interoperable blockchains. Medical IoT devices can encrypt and store real-time PHRs in an InterPlanetary File System, requiring only simple operations for data sharing. An enhanced proxy re-encryption(PRE) algorithm addresses the differences in blockchain cryptosystems. Multi-dimensional analysis demonstrates that this scheme offers robust security and excellent performance.**

***Index Terms*—cross-chain, data sharing, PHR, PRE**

I. Introduction

The widespread adoption of medical informatization has led to the creation of numerous Personal Health Records (PHR), these records contain sensitive physiological data parameters and patient medical histories, emphasizing high privacy concerns [1]. However, due to insecure current sharing mechanisms and unclear data rights and responsibilities, medical institutions that collect PHRs often operate as isolated data silos, limiting the full potential utilization of PHRs' value [2]. As blockchain technology gains popularity, more medical institutions are leveraging it to enhance data-sharing capabilities, aiming to address issues such as single points of failure and trust between different institutions during data sharing [2] [4] [5] [6] [7]. However, the above solutions primarily focus on data sharing within the same blockchain network, neglecting scenarios where medical institutions operate on different blockchains.

We illustrate the real need for cross-chain sharing of PHRs with an example. When Alice was hospitalized at Hospital A (on blockchain A), her PHRs were continuously collected via the hospital A's medical IoT devices. Due to the limited storage and computational capabilities of this equipment, Alice's PHRs were encrypted using her private key and sent to Hospital A's InterPlanetary File System (IPFS) for storage [1] [7]. Later, when Alice seeks treatment at Hospital B, Doctor Bob needs access to her previous PHRs from Hospital A. Since Hospitals A and B are on different blockchains, this scenario requires cross-chain PHR sharing. The main challenges in sharing PHRs across chains are: 1) Different blockchains typically employ distinct encryption mechanisms. 2) PHR is encrypted and stored on IPFS, with cross-chain sharing of PHR necessitating complex procedures [2] [4] [7]. 3) The cross-chain data sharing faces external attacks [8] [9].

Existing research often treats blockchain as a trusted entity for achieving medical data sharing through various encryption technologies. Wang et al. [5] proposed a decentralized electronic medical record-sharing framework called MedShare, which designed a constant-size attribute-based encryption (ABE) scheme to achieve fine-grained access control. Quan et al. [2] proposed a reliable medical data-sharing framework in an edge computing environment, addressing the challenges of real-time, multi-attribute authorization in ABE through a blockchain-based distributed attribute authorization strategy (DAA). Banik et al. [6] utilized public key encryption with keyword search (PEKS) technology to design a federated blockchain with preselected users, achieving data security, access control, privacy protection, and secure search. Liu et al. [4] combined ABE and searchable encryption (SE) to propose a multi-keyword search-based data-sharing scheme, providing comprehensive privacy protection and efficient ciphertext retrieval for electronic medical records. Zhao et al. [14] proposed a large-scale, verifiable and privacy-preserving dynamic fine-grained access control scheme based on attribute-based proxy re-encryption (PRE). The PRE algorithm is widely used in existing data sharing schemes [3] [8]. However, the cryptographic systems among different medical institutions can vary significantly. The encryption algorithms in [5] [2] [6] [4] [14] [3] [8] assume uniform cryptographic mechanisms, making them unsuitable for real medical scenarios.

To address these challenges, this paper enhances the proxy re-encryption algorithm from [9], enabling PHRs ciphertext to be converted and decrypted between Identity-Based Encryp-

tion (IBE) and Certificateless Cryptography (CLC) systems. Based on this improvement, we develop a cross-chain sharing scheme for PHR. In this scheme, real-time generated PHRs are encrypted and stored in the IPFS. When data sharing is required, IoT terminal devices with limited storage and computational capabilities can facilitate PHR sharing by utilizing smart contracts. The main contributions of this paper are as follows:

1) We introduce an enhanced proxy re-encryption algorithm capable of facilitating data sharing between IBE and CLC.
2) Building upon the enhanced proxy re-encryption algorithm, we present a scheme for cross-chain PHR sharing.
3) Security and performance evaluations demonstrate that the proposed scheme not only meets stringent security criteria but also exhibits superior operational efficiency.

II. Preliminaries

This section introduces the concepts of bilinear pairings, which are essential for constructing the scheme described in Section III-B.

A. Bilinear Pairing

Let G_1 and G_2 be two multiplication groups of order prime q, with g as the generator of G_1. A bilinear pairing $e: G_1 \times G_1 \rightarrow G_2$ satisfies the following properties:

1) Bilinearity: For $\forall (g_1, g_2) \in G_1, \forall (a, b) \in Z_q^*$, it must hold that $e\left(g_1^a, g_2^b\right) = e\left(g_1, g_2\right)^{ab}$.
2) Non-degeneracy: For $\exists (g_1, g_2) \in G_1$ and 1_{G_2} be the identity element of G_2, there have $e(g_1, g_2) \neq 1_{G_2}$.
3) Computability: For $\forall (g_1, g_2) \in G_1$, there exists an effective algorithm to compute $e(g_1, g_2)$.

III. Construction

This section provides a detailed explanation of the system model and the scheme's implementation.

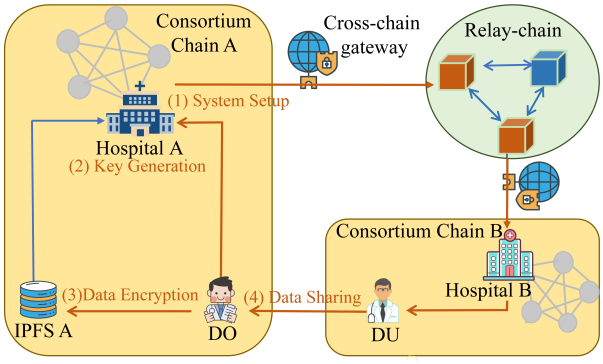


Fig. 1: The Scheme Model

A. System Model

In the scheme, we assume that there is a node, Hospital_A, in consortium chain A, which uses IBE as its cryptographic system. Similarly, there is a node, Hospital_B, in consortium chain B, which uses CLC as its cryptographic system. This scheme assumes that a data user in Hospital_B needs to access some PHRs from a data owner in Hospital_A. The scheme model is shown in **Fig. 1**, and the scheme includes the following entities:

Hospital (Hospital_i): A node in the blockchain that generates keys for users within the chain.

Data Owner (DO): A user in Hospital_A who owns the PHR.

Data User (DU): A user in Hospital_B who can be a patient, doctor, researcher, or any other person needing to use PHR.

Relay Chain: It provides computing power and is responsible for the calculation of re-encrypted ciphertext.

Interplanetary File System (IPFS_i): A semi-trusted distributed database responsible for storing PHRs to reduce the storage burden on IoT terminal devices.

B. Scheme Construction

This section introduces the details of the scheme's implementation.

1) System Setup: At this stage, consortium chains A and B register their systems to generate system parameters.

(1.1) Given a security parameter k, the Hospital_A in consortium chain A selects $s \in Z_q^*$ as the master private key and calculates the system public key $h_1 = g^s$, where g is the generator of G_1. Hospital_A public parameters $par_1 = \{G_1, G_2, e, g, h_1, H_1, H_2\}$.

(1.2) Similarly, Hospital_B in consortium chain B randomly selects $y \in Z_q^*$ as the master private key and calculates the system public key $h_2 = g^y$, public the parameters to $par_2 = \{G_1, G_2, e, g, h_2, H_1, H_2\}$.

2) Key Generation: At this stage, consortium chains A and B generate keys for users in their respective chains.

(2.1) Hospital_A generates the user's public key $pk_{DO} = H_1(ID_{DO})$ and private key $sk_{DO} = pk_{DO}^s$, and sends sk_{DO} to the DO.

(2.2) Hospital_B generates the user's partial private key $D_{DU} = H_1(ID_{DU})^y$. Hospital_B sends D_{DU} to the DU. The DU randomly selects $r \in Z_p^*$, calculates the private key $sk_{DU} = (D_{DU})^r = H_1(ID_{DU})^{yr}$, and the public key $pk_{DU} = (pk_{DU1}, pk_{DU2}) = (H_1(ID_{DU}), (h_2)^r)$.

3) Data Encryption: At this stage, the DO encrypts PHR and uploads it to IPFS_A for storage.

(3.1) The DO selects the message M (containing PHR) to be shared, given par_1 and pk_{DO}, randomly selects $\alpha \in Z_q^*$, and generates the ciphertext $C_{DO} = (c_1, c_2)$, $c_1 = g^\alpha, c_2 = M \cdot e(h_1, pk_{DO})^\alpha$. Then, the DO sends C_{DO} and its identifier $Data_1$ to IPFS_A for storage.

(3.2) Simultaneously, Hospital_A saves the ciphertext identifier $Data_1$ and its address Add_1 in the access list $List_1$.

4) Data Sharing: At this stage, the DU initiates a cross-chain access request to the DO. After successfully verifying the request message, the DO shares the data with the DU.

(4.1) To access the message M from the DO, the DU must first send a cross-chain access request message $M_1 = \{request_1, pk_{DO}, pk_{DU}, T_1, N_1\}_{pk_{DO}}$. Here, $request_1$ is the cross-chain access identifier, T_1 is the timestamp,

and N_1 is the nonce to maintain session freshness. The message M_1 is forwarded to the DO via the cross-chain gateway.

(4.2) Upon receiving the request, the DO verifies the validity of the message and the correctness of the DU's identity. If the verification is successful, the DO randomly selects λ and X. Then, using its own private key sk_{DO} and the DU's public key pk_{DU}, the DO generates the re-encryption key $rk_{DO} = (rk_1, rk_2, rk_3)$, $rk_1 = H_2(X)/sk_{DO}, rk_2 = g^{\lambda}, rk_3 = X \cdot e(pk_{DU1}, pk_{DU2})^{\lambda}$, and sends it to Hospital_A.

(4.3) The DO then sends the ciphertext identifier $Data_1$ and the cross-chain data sharing permission message $M_2 = \{request_2, pk_{DO}, pk_{DU}, rk_{DO}, T_2, N_2\}$ to Hospital_A. Hospital_A ultimately sends M_2 and the ciphertext C_{DO} to the relay chain.

(4.4) The relay chain generates the re-encrypted ciphertext $C_{DU} = (C_1, C_2, C_3, C_4)$ based on the given C_{DO} and rk_{DO}, $C_1 = c_1, C_2 = c_2 \cdot e(C_1, rk_1), C_3 = rk_2, C_4 = rk_3$. Finally, the relay chain sends the response message $M_3 = \{respond_1, C_{DU}, T_3, N_3\}$ to the DU via the cross-chain gateway.

(4.5) Upon receiving the response message M_3, the DU first verifies the validity of the message. After successful verification, the DU uses its private key sk_{DU} to calculate $X = C_4/e(C_3, sk_{DU})$, and then calculates $M = C_2/e(C_1, H_2(X))$ to obtain the message M.

C. Scheme Correctness Proof

We check whether the DU has accurately decrypted the re-encrypted ciphertext $C_{DU} = (C_1, C_2, C_3, C_4)$.

$$\begin{aligned}\frac{C_4}{e\left(C_3, sk_{DU}\right)} &= \frac{rk_3}{e\left(rk_2, sk_{DU}\right)} \\ &= X \cdot \frac{e(pk_{DU1}, pk_{DU2})^{\lambda}}{e(g^{\lambda}, sk_{DU})} \\ &= X \cdot \frac{e(H_1\left(ID_{DU}\right), g^{yr})^{\lambda}}{e(g^{\lambda}, H_1\left(ID_{DU}\right)^{yr})} \\ &= X\end{aligned}$$

It is evident that X can be correctly decrypted by DU.

$$\begin{aligned}\frac{C_2}{e\left(C_1, H_2\left(X\right)\right)} &= \frac{c_2 \cdot e(c_1, rk_1)}{e(c_1, H_2(X))} \\ &= M \cdot \frac{e\left(g^s, pk_{DO}\right)^{\alpha} \cdot e(g^{\alpha}, H_2(X))}{e\left(g^{\alpha}, H_2\left(X\right)\right) \cdot e(g^{\alpha}, sk_{DO})} \\ &= M \cdot \frac{e\left(g^s, pk_{DO}\right)^{\alpha}}{e\left(g^{\alpha}, pk_{DO}^{s}\right)} \\ &= M\end{aligned}$$

Based on the correct decryption of X, the DU also correctly decrypts the ciphertext C_{DU} to obtain message M.

IV. Safety Analysis

In this section, we prove that the scheme meets CPA security. We references the security model played by the challenger $\mathcal{C}$ and the adversary $\mathcal{A}$ in [9], which is detailed as follows:

Theorem 1. The KGC of the data owner in this scheme preserve weak security and resist weak exfiltration. Here, preserving weak security means that Ateniese's [12] IBPRE scheme is CPA secure. Resisting weak exfiltration means that when faced with an adversary launching an ASA that does not affect normal functionality, this scheme can resist information leakage.

Proof. Similar to the proof method in [9], our constructed scheme also achieves CPA security.

V. Performance Analysis

In this section, we evaluate the computational and communication overhead. Experiments were conducted on a Lenovo laptop with an AMD Ryzen 7 5800H processor with Radeon Graphics running at 3.20 GHz and 16GB of RAM. The host machine runs Ubuntu 22.04.2 operating system, with Java 1.8.0_102, and employs FISCO-BCOS blockchain v3.6.0.

A. Computational Overhead

We calculate the computational overhead of core operations in the schemes, focusing on computationally expensive operations such as bilinear pairing, exponentiations in the group G_1 and G_2, and hash function computations. We chose to compare our scheme with [10] [11] and [13] because they, like ours, achieve encryption system transformation through proxy re-encryption. Notably, [10] first introduced the concept of encryption system transformation.

As shown in **Fig. 2**(a), as the number of users increases, our scheme exhibits a greater advantage in the time required to complete all users' **Enc** operations. As depicted in **Fig. 2**(b), we combine the **ReKeyGen** and **ReEnc** operations into a single **query** operation, the advantage in the time required to complete all **query** operations becomes more significant as the number of users increases. Thus, compared with [10] [11] [13], our scheme demonstrates more efficient performance under higher user loads.

B. Communicational Overhead

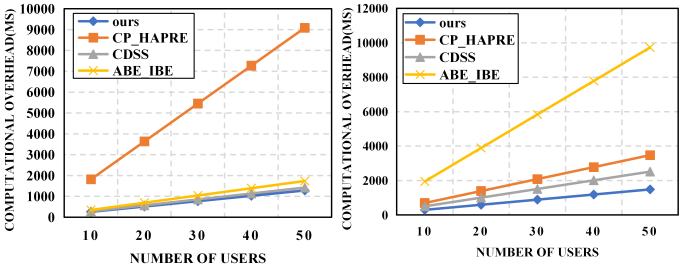
Regarding communication overhead, during system operation, it is necessary to transmit and receive key pairs (**Key**), ciphertexts (**CT**), re-encryption keys (**RK**), re-encrypted ciphertexts (**CT'**), and other primary data. The lengths of these data are directly related to the size of communication overhead during system operation. Therefore, We calculate the number of elements contained in the G_1, G_2 and Z_q group, which are part of the core data of the scheme, to evaluate their communication overhead. It is important to note that the CP-HAPRE and ABE-IBE schemes involve ABE. For fairness in experiments, we use the simplest access policy in ABE, setting the total number of attributes (**N**) in the access policy to 5 and the number of attributes required for access (**n**) to 3.

As shown in **Table I**, our scheme enhances system security while maintaining an advantage in communication overhead. Regarding the key **Key**, on average, each key pair in our

TABLE I: Comparison of Communicational Overhead

Scheme	Key$_{DO}$	Key$_{DU}$	CT	RK	CT'	Total(bytes)
CP-HAPRE [11]	(2n+4)$\|G_1\|$	(2n+4)$\|G_1\|$	(3N+2)$\|G_1\|$+$\|G_2\|$	7$\|G_1\|$	4$\|G_1\|$+$\|G_2\|$	4864
CDSS [13]	6$\|G_1\|$+2$\|Z_q\|$	7$\|G_1\|$+2$\|Z_q\|$	3$\|G_1\|$+2$\|G_2\|$	4$\|G_1\|$+$\|G_2\|$	$\|G_1\|$+3$\|G_2\|$	2408
ABE-IBE [10]	(2N+1)$\|G_1\|$	2$\|G_1\|$	(N+1)$\|G_1\|$+$\|G_2\|$	(4N+3)$\|G_1\|$+$\|G_2\|$	2$\|G_1\|$+$\|G_2\|$	4928
Ours	2$\|G_1\|$	3$\|G_1\|$	2$\|G_1\|$+$\|G_2\|$	2$\|G_1\|$+$\|G_2\|$	2$\|G_1\|$+2$\|G_2\|$	1344

$|G_1|$: Storage overhead of group elements in G_1(128bytes) $|G_2|$: Storage overhead of group elements in G_2(128bytes)
$|Z_q|$: Storage overhead of group elements in Z_q(20bytes)



(a) The Computational Overhead of Multi-User Enc Operations (b) The Computational Overhead of Multi-User Query Operations

Fig. 2: Comparison of Computational Overhead

scheme only contains 2.5 elements from the G_1 group. For the ciphertext **CT**, our scheme requires only 2 elements from the G_1 group and 1 element from the G_2 group for ciphertext generation, which contrasts favorably with other schemes. Concerning the re-encryption key **ReKey**, our scheme needs just 2 elements from the G_1 group and 1 element from the G_2 group for key generation. As for the re-encrypted ciphertext **CT'**, communication overhead is generally consistent across all schemes. Therefore, compared with [10] [11] [13], our scheme can effectively save communication overhead when the number of users increases.

VI. Conclusion

This paper proposes a cross-heterogeneous chain data sharing scheme tailored for the medical context. It addresses the limitations of storage and computing resources in medical IoT devices and facilitates PHRs sharing through IBE and CLC. The proposed scheme enhances security measures effectively. In the future, we plan to undertake more in-depth research on internal attacks within cross-chain environments to enhance the security of cross-chain protocols. Additionally, we aim to optimize the performance of cross-chain schemes to ensure compatibility with resource-constrained devices, such as those in the internet of medical things.

Acknowledgment

This work was supported by the National Key Research and Development Program of China (2021YFF1201102).

References

[1] Z. Bao, D. He, H. Wang, M. Luo, and C. Peng, "A group signature scheme with selective linkability and traceability for blockchain-based data sharing systems in e-health services," IEEE Internet of Things Journal, 2023.

[2] G. Quan, Z. Yao, L. Chen, et al., "A trusted medical data sharing framework for edge computing leveraging blockchain and outsourced computation," Heliyon, vol. 9, no. 12, 2023.

[3] C. Ren, X. Dong, J. Shen, Z. Cao, and Y. Zhou, "Clap-pre: Certificateless autonomous path proxy re-encryption for data sharing in the cloud," Applied Sciences, vol. 12, no. 9, p. 4353, 2022.

[4] J. Liu, Y. Fan, R. Sun, L. Liu, C. Wu, and S. Mumtaz, "Blockchain-aided privacy-preserving medical data sharing scheme for e-healthcare system," IEEE Internet of Things Journal, 2023.

[5] M. Wang, Y. Guo, C. Zhang, C. Wang, H. Huang, and X. Jia, "Medshare: A privacy-preserving medical data sharing system by using blockchain," IEEE Transactions on Services Computing, vol. 16, no. 1, pp. 438–451, 2021.

[6] M. Banik and S. Kumar, "Blockchain-based public key encryption with keyword search for medical data sharing in cloud environment," Journal of Information Security and Applications, vol. 78, p. 103 626, 2023.

[7] D. Kumari, A. S. Parmar, H. S. Goyal, K. Mishra, and S. Panda, "Healthrec-chain: Patient-centric blockchain enabled ipfs for privacy preserving scalable health data," Computer Networks, p. 110 223, 2024.

[8] Y. Zhou, J. Guo, and F. Li, "Certificateless public key encryption with cryptographic reverse firewalls," Journal of Systems Architecture, vol. 109, p. 101 754, 2020.

[9] Y. Zhou, L. Zhao, Y. Jin, and F. Li, "Backdoor-resistant identity-based proxy re-encryption for cloud-assisted wireless body area networks," Information Sciences, vol. 604, pp. 80–96, 2022.

[10] T. Mizuno and H. Doi, "Hybrid proxy re-encryption scheme for attribute-based encryption," in Information Security and Cryptology: 5th International Conference, Inscrypt 2009, Beijing, China, December 12-15, 2009. Revised Selected Papers 5, Springer, 2010, pp. 288–302.

[11] H. Deng, Z. Qin, Q. Wu, Z. Guan, and Y. Zhou, "Flexible attribute-based proxy re-encryption for efficient data sharing," Information Sciences, vol. 511, pp. 94–113, 2020.

[12] M. Green and G. Ateniese, "Identity-based proxy re-encryption," in Applied Cryptography and Network Security: 5th International Conference, ACNS 2007, Zhuhai, China, June 5-8, 2007. Proceedings 5, Springer, 2007, pp. 288–306.

[13] P. Jiang, J. Ning, K. Liang, C. Dong, J. Chen, and Z. Cao, "Encryption switching service: Securely switch your encrypted data to another format," IEEE Transactions on Services Computing, vol. 14, no. 5, pp. 1357–1369, 2018.

[14] J. Zhao, K. Zhang, J. Gong and H. Qian, "Lavida: Large-Universe, Verifiable, and Dynamic Fine-Grained Access Control for E-Health Cloud," in IEEE Transactions on Information Forensics and Security, vol. 19, pp. 2732-2745, 2024