Blockchain-assisted Revocable Hierarchical Attribute-based Encryption Electronic Medical Record Sharing Scheme

Xiaotao Yang*, Zaibin Chang, Man Jiang
Public Course Department, Xi'an Traffic Engineering Institute, Xi'an, Shaanxi, China
**Corresponding Author.*

Abstract: The integration of modern medical systems with the internet of things has significantly improved medical services. Nevertheless, the widespread outsourcing of electronic medical records to third-party cloud storage introduces numerous security challenges, including privacy breaches, data tampering, unauthorized access, and storage limitations. To mitigate these issues, this paper introduces a novel blockchain-assisted revocable hierarchical attribute-based encryption scheme for electronic medical record sharing. This scheme leverages a decentralized blockchain system to manage user revocation and key management tasks, thereby alleviating the need for user ciphertext re-encryption. Additionally, employing ciphertext policy attribute-based encryption enhances access control granularity and safeguards user privacy by concealing access policies. Performance analysis indicates superior performance of the proposed scheme.

Keywords: Internet of Things; Electronic Medicalrecords; Blockchain Technology; Attribute-based Encryption; Access Control

1. Introduction

As science and technology advance rapidly, mechanization and intelligent equipment are increasingly substituting labor-intensive human tasks, significantly enhancing people's lives. Smart Healthcare exemplifies this progress, offering telemedicine services amid the ongoing coronavirus disease pandemic. These services not only minimize direct interactions between doctors and patients, thereby lowering the risk of cross-infection, but also enhance the accessibility of medical resources. Consequently, costs decrease, and medical services become more efficient.

In today's landscape, cloud computing technology offers myriad advantages, prompting a growing number of electronic medical records to be outsourced and stored in third-party cloud service providers (CSP). This approach enables users to efficiently store and access their electronic medical records (EHRs), thus enhancing the overall efficiency of medical services. However, within cloud computing, concerns regarding data privacy disclosure have emerged as a significant issue. Consequently, users must encrypt their data before sharing it. Conventional encryption schemes, as delineated by Sahai et al. [1], often lead to complex key escrow problems, resulting in substantial storage overhead. Consequently, conventional one-to-one encryption methods fall short of meeting users' access control requirements. In recent years, fine-grained attribute-based encryption (ABE) has gained significant attention in the field of cryptography. This essay aims to explore the concept of fine-grained ABE as proposed by Goyal [2] and its implications.The ciphertext policy ABE (CP-ABE) scheme, particularly suitable for the medical system according to Xiang et al. [3], represents a flexible and viable encryption solution for diverse scenarios. Ciphertext policy-based attribute encryption (CP-ABE) stands as a promising public key encryption scheme within cloud computing, as highlighted by Liu et al. [4]. It enables the embedding of access control policies in ciphertext, thereby facilitating flexible data control. The pioneering ABE scheme, introduced in 2007 by Bethencourt et al., represented a novel public key encryption system capable of one-to-many encryption, specifically suited for medical systems. However, in the aforementioned ABE scheme, the challenge arises when users share multiple Electronic Health Records (EHRs), necessitating the definition of multiple access structures and multiple encryptions of these EHRs. This not only escalates time consumption but also occupies a substantial

amount of cloud storage space. To address this issue, Wang et al. [5] proposed an ABE scheme based on the file level in cloud computing. This scheme, as depicted in Figure 1, consolidates hierarchical access structure sets into a unified access structure and subsequently encrypts hierarchical files using the combined access structure, thus optimizing ciphertext storage space and enhancing encryption efficiency. However, the efficacy of these scenarios heavily relies on Cloud Service Providers (CSPs). Conversely, CSPs may delete data that users infrequently access to make room for other users' data, potentially resulting in financial gains. Nevertheless, data stored in the cloud is vulnerable to corruption due to cloud server failures, administrative errors, or malicious attacks. Moreover, CSPs may intentionally obscure data losses to safeguard their reputation. Consequently, while the cloud facilitates the seamless sharing of electronic medical data among medical institutions, it also exposes such data to manipulation, forgery, and unauthorized access. Blockchain emerges as a novel internet database technology characterized by decentralization, transparency, and immutable data, among other attributes. Proposed initially by Nakamoto in [6], blockchain's integration into the medical system obviates the necessity for third-party data storage and mitigates the risk of data tampering. Consequently, it offers a viable solution to circumvent cloud data security concerns. The application of blockchain in the medical domain has garnered significant scholarly attention in recent years, extending its utility beyond healthcare to fields such as finance, communication, and the Internet of Things (IoT).

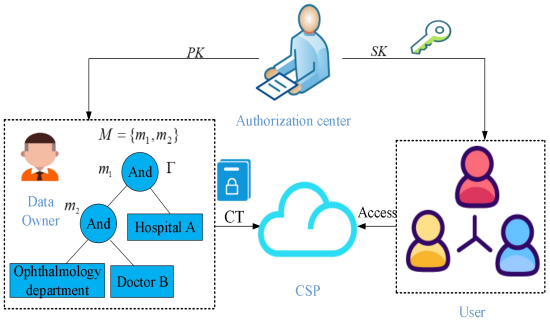

Figure 1. Medical Record Sharing in Cloud Computing

In this paper, we introduce a novel blockchain-assisted revocable hierarchical attribute-based encryption (BC-RHABE) scheme for secure electronic medical record (EMR) storage and sharing. Our contributions can be outlined as follows:

(1) Decentralized scheme: We present a decentralized approach where a blockchain system replaces the centralized authority for tasks like key management, threshold parameter generation, and user revocation. By leveraging blockchain technology, all revocation tasks are efficiently managed, reducing the burden of user ciphertext re-encryption and ensuring the integrity of data storage.

(2) Enhanced data confidentiality: Our scheme ensures the confidentiality of medical data through advanced encryption techniques and hierarchical access tree structures. By employing fine-grained access controls, files are encrypted using a hierarchical structure, optimizing storage space utilization, and safeguarding user privacy.

(3) Low computing overhead: We address the computational overhead associated with decryption operations by outsourcing them to cloud servers. The proposed approach significantly alleviates the decryption burden on users, while simultaneously ensuring the accuracy and completeness of medical data through the implementation of dual verification protocols.

(4) Security and efficiency analysis: Through rigorous efficiency analysis, we demonstrate that our scheme meets the security and efficiency requirements of blockchain-assisted key management in cloud storage environments. Our scheme is validated to be secure based on the decisional bilinear diffie-hellman (DBDH) hypothesis, ensuring robust protection against unauthorized access and data tampering.

2. Related Knowledge

2.1 Bilinear Maps

Let G_1 and G_2 be two cyclic groups of same prime order p. The generator of G_1 is g. A bilinear mapping $e: G_1 \times G_1 \to G_2$ satisfies the following properties:

(1) Bilinearity: For any $u, v \in G_1$ and $a, b \in Z_p^*$, it has $e(u^a, v^b) = e(u, v)^{ab}$.

(2) Non-degeneracy: There exists $u, v \in G_1$ such $e(u, v) \neq 1$.

(3) Computability: For all $u, v \in G_1$ and $a, b \in Z_p$, there is an effective polynomial time algorithm to computation $e(u, v) \in G_2$.

2.2 Decisional Bilinear Diffile-hellman Assumption (DBDH)

Let G_0 be a group with prime order p, g be a generator in G_0. We say that DBDH assumption holds if no probabilistic polynomial time (PPT) adversary can distinguish the tuples $(g, A = g^a, B = g^b, C = g^c, e(g,g)^{abc})$ and $(g, A = g^a, B = g^b, C = g^c, e(g,g)^d)$, where $a, b, c, d \in Z_p$. The advantage of algorithm $\Re$ is

$$Adv_B^{DBDH} = |\Pr[\Re(A, B, C, e(g,g)^{abc}) = 0] - \Pr[\Re(A, B, C, e(g,g)^d) = 0]|$$

2.3 Hierarchical Access Tree

The hierarchical tree, as proposed by Wang et al. [5], is a consolidated access structure formed by multiple access structures, enabling the sharing of multiple hierarchical files.

3. Scheme Model

As depicted in Figure 2, the primary entities within this scheme system include the Data Owner (DO), Data User (DU), Blockchain (BC), and Cloud Service Provider (CSP).

(1) The Data Owner (DO) is responsible for sharing and storing a significant volume of encrypted data in the cloud server. In this scheme, the DO's primary tasks involve defining the access structure and authentication key. Additionally, the DO utilizes encryption algorithms to encrypt the data file and subsequently uploads the encrypted ciphertext and authentication key to the cloud server.

(2) Data User (DU): the user accesses the ciphertext data in the cloud storage and downloads the ciphertext he/she is interested in. If the user attribute set meets the access structure, the decryption algorithm of the scheme is used to decrypt the corresponding symmetric key, then the symmetric key is used to decrypt the corresponding plaintext information.

(3) Blockchain (BC): A distributed ledger that records the process of data sharing in the system and the fine-grained authorization process. Blockchain records the mapping relationship between DU and its attribute set, and publishes the change of user attribute state and the description information of shared data, thus ensuring the security, imtamability and auditability of data sharing. In addition, all the consensus nodes work together to update the user revocation list.

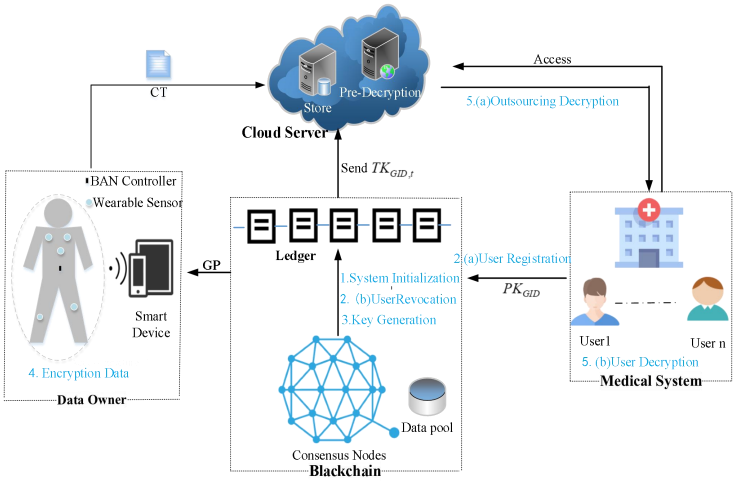

Figure 2. Our Scheme Model

(3) Cloud service provider (CSP): In the system, it is a trusted entity, but it is curious. In this scheme, its main tasks are ciphertext storage, pre-decryption, and transmission services for users.

4. Peformance Analysis

In this section, our scheme conducts a comprehensive evaluation of its programs [5, 7-12] in terms of function. In addition, the performance of this scheme is compared with that of other schemes [10-12] in terms of storage cost. Through analysis, it is found that although this scheme is a multi-authority ABE scheme, it does not need authorization key and consensus node as authority, but generates parameters through Pedersen (k, n) secret sharing protocol, without private key or public

key. In this scheme, the user private identity key acts as the user decryption key. Table 1 shows the symbols used in performance analysis.

Table 1. Symbol definitions

symbol	Definition
L_*	the bit-length of element in $*$
l	the number of files
S_i	the least interior nodes satisfying Γ
A_u	the attributes set of User u
A_{c_i}	the attributes related with ciphertext
A_T	the set of transport nodes
$\|*\|$	the number of elements in $*$

4.1 Functional Comparison

Table 2 shows the comparison of functions between our scheme with schemes [5,7-12] are all CP-ABE type. Compared with the hierarchical attribute-based encryption (ABE) scheme [5,10], these schemes use decentralized blockchain system replaces the authority center, which avoids the CSP tampered data problem; Besides, user all revocation tasks are completed by blockchain, thus reducing the burden of user ciphertext re-encryption and key re-updating. However, in scheme [5], it only uses a single authority to manage the key, which is caused key escrow problems as the number of users increases; In addition, the scheme [5] does not implement ciphertext integrity verification and policy hiding, which may easily lead to the possibility of message tampering. Compared with our scheme, scheme [10] uses multi-authoritative attribute-based encryption technology and has the functions of integrity verification and policy hiding, but scheme [10] does not apply blockchain decentralization, transparency, and data immutable technology, which may easily cause data message tampering. In addition, there is no key revocation and outsourcing decryption functions, so it is easy to cause the system information to be destroyed by external users and users to decrypt the problem of high cost. Therefore, our scheme is more feasible in the medical system.

4.2 Storage Cost

As shown in Table 3, the storage sizes of master key, pre-decrypted key, decrypted key and ciphertext are mainly compared between this scheme and scheme [10-12]. According to data analysis, with the increase of files number and attribute number, the space occupied by private key and ciphertext increases significantly. Scheme [10-12] he size of key and ciphertext increases more. Therefore, this scheme costs less in storage overhead.

Table 2. Function Comparison of ABE scheme

scheme	type	Access structure	Block chain-aided	Multi-authority	Integrity verification	revocable	Policy hidden	outsource decryption
[11]	CP-ABE	Access tree	×	×	×	×	×	×
[7]	CP-ABE	LSSS	×	√	×	×	√	×
[9]	CP-ABE	And gate	×	√	×	×	√	×
[8]	CP-ABE	LSSS	×	√	√	×	√	√
[12]	CP-ABE	LSSS	√	√	×	√	×	×
[5]	FH-CP-ABE	Hierarchical access tree	×	×	×	×	×	×
[10]	FH-CP-ABE	Hierarchical access tree	×	√	√	×	√	×
Ours	FH-CP-ABE	Hierarchical access tree	√	√	√	√	√	√

Table 3. The Comparison of Storage Cost

Component	[11]	[12]	[10]	Ours
MSK	$L_{Z_p}+L_{G_0}$	-	$L_{Z_p}+L_{G_0}$	-
TK	-	$(2\|A_u\|+6)L_{G_0}$	-	$(3\|A_u\|+5)L_{G_0}$
SK	$2l(\|A_u\|+1]L_{G_0}$	$2l(\|A_u\|+2)L_{G_0}$	$2(2\|A_u\|+1)L_{G_0}$	$3(\|A_u\|+1)L_{G_0}$
CT	$[2(\|A_{C_1}\|+\cdots+\|A_{C_l}\|)+l]L_{G_0}+lL_{G_T}$	$[(\|A_{C_1}\|+\cdots+\|A_{C_l}\|)+5l]L_{G_0}+lL_{G_T}$	$(2\|A_{C_1}\|+l+1)L_{G_0}+(k'\|A_T\|+l)L_{G_T}$	$(\|A_{C_1}\|+2l+2)L_{G_0}+(k'\|A_T\|+l)L_{G_T}$

5. Conclusions

This study explores the application of ABE technology in modern healthcare systems and proposes a blockchain-assisted, reversible layered ABE electronic medical record sharing

scheme. Compared with aboriginal BC-SABE scheme, our solution utilizes a hierarchical access tree structure, providing fine-grained access control. Additionally, it improves encryption efficiency and saves storage space by encrypting multiple files simultaneously. Furthermore, the solution hides the access structure to protect user privacy. The decrypted plaintext information undergoes dual verification to ensure accuracy and integrity of medical data. Efficiency analysis demonstrates that this solution meets the security and efficiency requirements of blockchain-assisted key management in cloud storage environments and is considered secure under DBDH assumption. Implementing this solution will contribute to secure sharing of medical data. Future plans involve promoting this solution based on our paper and building a secure and practical data sharing system with payment functionality.

Acknowledgement

This paper is supported by Shaanxi Fundamental Science Research Project for Mathematics and Physics (No. 23JSQ058), the Young and Middle-aged fund project of Xi'an Traffic Engineering Institute under Grant (2023KY-53).

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

References

[1] A. Sahai, and B. Waters, Fuzzy identity-based encryption, Proc of International Conference on Theory and Applications of Cryptographic International Conference on Theory and Applications of Cryptographic Techniques. [S.l.]: Springer-Verlag, 2005, pp.457-473.

[2] V. Goyal, O. Pandey, A. Sahai, PV. Goyal, and PV. Sahai, Attribute-based encryption for fine-grained access control of encrypted data. Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006,Alexandria, VA, USA, loctober 30-November 3, 89-98,2006.

[3] Xiang, X, Y and Zhao, X, W. Blockchain-assisted searchable attribute-based encryption for e-health systems, Journal of Systems Architecture. March 2022, vol.124, pp.102417.

[4] X. Liu, Y. Xia, We. Yang, and F. Yang. Secure and Efficient Querying over Personal Health Records in Cloud Computing, Neurocomputing, 2018, Vol.274, pp: 99-105.

[5] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie. An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing, IEEE Transactions on Information Forensics and Security. 2016, 11(6): 1265-1277.

[6] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Accessed: 2008.

[7] P. Liang, L. Zhang, L. Kang, and Juan Ren, "Privacy-preserving decentralized ABE for secure sharing of personal health records in cloud storage," Journal of Information Security and Applications, vol. 47, 2019, pp. 258–266.

[8] S. Belguith, N. Kaaniche, M. Laurent, A Jemai, and R. Attia, "PHOABE: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT," Computer Networks, vol.133, 2018, pp. 141–156.

[9] H. Qian, J. Li, and Y. Zhang, "Privacy-Preserving Decentralized Ciphertext-Policy Attribute-Based Encryption with Fully Hidden Access Structure," Springer International Publishing Switzerland, pp. 363–372, 2013.

[10] X. Liu, X. Yang, Y. Luo, L. Wang, and Q. Zhang. Anonymous Electronic Health Record Sharing Scheme Based on Decentralized Hierarchical Attribute-Based Encryption in Cloud Environment, IEEE Access, vol.8, 2020. pp, 200180-200193.

[11] J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-policy attribute based encryption, IEEE Symposium on Security and Privacy, pp. 321–334, May 2007.

[12] Suhui Liu, Jiguo Yu, Yinhao Xiao, Zhiguo Wan, Shengling Wang, Biwei Yan. "BC-SABE: Blockchain-aided Searchable Attribute-based Encryption for Cloud-IoT", IEEE Internet of Things Journal, 2020.pp.1-1.

