Hindawi
IET Information Security
Volume 2024, Article ID 2498245, 14 pages
https://doi.org/10.1049/2024/2498245

Research Article

HA-Med: A Blockchain-Based Solution for Sharing Medical Data with Hidden Policies and Attributes

Xiaohui Yang and Jing Liu

School of Cybersecurity and Computer Science, Hebei University, Baoding, China

Correspondence should be addressed to Jing Liu; 2251881634@qq.com

Received 16 June 2023; Revised 14 February 2024; Accepted 15 April 2024; Published 26 April 2024

Academic Editor: Hyun-A Park

Existing healthcare data-sharing solutions often combine attribute-based encryption techniques with blockchain technology to achieve fine-grained access control. However, the transparency of blockchain technology may introduce potential risks of exposing access structures and user attributes. To address these concerns, this paper proposes a novel healthcare data-sharing scheme called HA-Med. By leveraging blockchain technology, HA-Med ensures the concealment of access policies and attributes, providing a secure solution for fine-grained access control of medical data. Furthermore, the scheme supports attribute revocation and forward secrecy to enhance user privacy. The security of HA-Med is rigorously verified through theoretical analysis, and its feasibility is demonstrated through experiments conducted using the Java-based JPBC library.

1. Introduction

Due to the rapid development of the Internet, the medical field has undergone tremendous changes, and electronic health records [1] have become widely used. Electronic health records encompass patients' treatment records, condition status, and other medical documentation generated during treatment. They enable medical staff to easily access a patient's past medical history online. However, with the increasing popularity of electronic health records [2], it has become increasingly challenging to store electronic medical records in hospitals due to the varying storage models. Additionally, integrating a patient's medical data across different hospitals has proven difficult, leading to the introduction of cloud storage [3] as a solution to these issues. Nonetheless, the adoption of cloud storage has given rise to numerous privacy and security concerns, as many services are outsourced to third parties due to the semi-trusted nature of cloud service providers. When a patient uploads data to the cloud, the data are no longer under the direct control of the data owner, potentially resulting in tampering and significant data loss. Furthermore, if a malicious user tampers with a patient's medical data, it may be challenging to trace the source of the tampering [4, 5].

In recent years, attribute-based encryption (ABE) has been widely used in healthcare in combination with cloud storage because of its ability to protect the privacy of data and to have fine-grained access control [6, 7]. According to the role of the access control policymaker, ABE can be divided into two categories, which are key-based policy ABE (KP-ABE) and ciphertext-based policy ABE (CP-ABE) [8]. CP-ABE, since the policy is embedded in the ciphertext, means that the data owner can set the policy to decide which attributes of the people who have access to this ciphertext, which is equivalent to doing an encrypted access control to this data. Therefore, CP-ABE is more suitable than KP-ABE for electronic medical health record access [8].

Blockchain is decentralized, traceable, and transparent. Once data are on the chain, it cannot be tampered with and can be traced when malicious users perform malicious operations. This feature of blockchain can effectively protect the security of medical data and provide new ideas to solve the above problems [9, 10]. The combination of blockchain technology, cloud storage, and CP-ABE has now started to be applied to the medical field [11, 12].

But at the same time, a new problem arises. Due to the transparency characteristic of blockchain, the data on the chain can be viewed by all. When applying traditional

CP-ABE for fine-grained access, the access structure is explicitly sent along with the ciphertext, which can potentially allow untrusted third parties to access the explicit attributes of the user in the access policy [13] and consequently infer important information. Since medical data contain a large amount of sensitive information about patients, compromising these data can lead to significant damage.

1.1. Policy Hiding. The current work on hiding access policies takes two forms: complete hiding [14] and partial hiding [15]. Complete hiding means that the attributes in the access policy are concealed so that the access policy does not reveal any attributes. Partial hiding involves concealing sensitive attributes in the access policy [16]. It can be observed that in terms of efficiency, partial hiding is more efficient than complete hiding, but complete hiding provides better privacy protection. This is particularly important when ABE is applied to medical care, as medical data contain a lot of private patient information, and compromising these data can lead to irreparable harm to patients. Additionally, when the policy is hidden, a new problem arises in that the user also does not know the values of the attributes in the access policy, requiring a verification algorithm to determine whether the user's attribute set satisfies the access policy or not [13].

1.2. Attribute Hiding. Most current schemes involving ABE require the data user to provide a set of attributes used to obtain the key to an intermediate entity, such as an authority. However, if the intermediate entity is compromised, the attributes may be leaked, posing a significant threat to attribute privacy [17]. In this context, attribute privacy refers to the privacy of the user's attribute set. Therefore, it is necessary to implement attribute hiding in the ABE scheme.

Therefore, to address the aforementioned issues, this paper proposes a secure blockchain-based scheme for concealing policies and attributes in medical data sharing. We design a verification method that combines bilinear pairing and predicate encryption to achieve policy and attribute hiding, named HA-Med, which ensures secure access to medical data while safeguarding the privacy of users and patients.

The contribution of this paper is as follows:

(i) In this paper, we propose a novel, trusted, and secure access control scheme for medical data called HA-Med. HA-Med introduces a new authentication method that addresses the issue of access policy and attribute exposure during ABE, achieving complete policy concealment while satisfying the access requirements of large universes.

(ii) Combining the blockchain with the authentication method proposed by the scheme resolves the issue of distributing permissions by a third party in traditional ABE, while simultaneously addressing the problem of overburdening the user with computation and storage in schemes that eliminate the third party.

(iii) The security of the proposed scheme was demonstrated theoretically, and its effectiveness was validated through comprehensive experiments.

2. Related Work

2.1. Blockchain. Blockchain has been widely used in healthcare over the years due to its anonymity and immutability. Ivan [18] proposed that blockchain can be used as a method to secure health data storage. Chen et al. [19] proposed a personal healthcare data storage scheme based on blockchain and cloud storage. Ekblaw et al. [20] proposed a blockchain-based electronic health record management system called MedRec. Xia et al. [21] proposed a blockchain-based data-sharing framework called BBDS. Dagher et al. [22] proposed a secure blockchain-based medical record-sharing framework called Ancile, which employs smart contracts to enhance the access control functionality. Dubovitskaya et al. [23] proposed a blockchain-based framework for cancer patient care to manage and share EMR data. However, these solutions suffer from the problem of not having fine-grained access to the data. Zheng et al. [24] proposed a blockchain-based attribute encryption access control scheme in which an access control model with multiple authorization authorities is established. Sun et al. [25] proposed a blockchain-based case data-sharing model supporting fine-grained access, and this model uses ABAC to realize fine-grained access to cases in research institutions. Han et al. [26] proposed a traceable access control scheme for medical attribute passes to achieve traceability of the access process. However, although the above scheme realizes the fine-grained access control of medical data, the policies and attributes are not hidden, which exposes the user's privacy.

2.2. CP-ABE. ABE has also been widely used in recent years as it provides fine-grained access to data. Riad et al. [27] proposed an access control mechanism that adaptively assigns appropriate permissions based on user roles. Wei et al. [28] proposed an encryption method based on revocable storage hierarchical attributes. Pournaghi et al. [12] proposed a scheme for medical data sharing called MedSBA. This scheme is based on blockchain, CP-ABE, and KP-ABE. Liu et al. [29] proposed a blockchain-assisted searchable ABE scheme with efficient undo performance. Deb et al. [11] proposed a scheme that combines blockchain and property-based encryption to preserve information about patients suffering from a novel coronavirus. Guo et al. [30] proposed an outsourced and online/offline revocable ciphertext policy attribute encryption scheme for medical Internet applications. However, although the above schemes can achieve fine-grained access to medical data, an attacker can infer many privacy attributes from the access policy in the ciphertext, which can lead to the exposure of patients' sensitive privacy. Li et al. [31] proposed a controlled and regulated privacy protection scheme for blockchain multiorganizational transactions based on attribute encryption. This scheme achieves fine-grained access control but suffers from the problem of distributing attributes by third-party authoritative centers, which distribute attributes to the members of the system, creating a corresponding privacy and security problem. Feng et al. [32] proposed a blockchain data-sharing scheme based on localized differential privacy and attribute-based searchable encryption, which can withstand attacks from untrustworthy third parties.

However, the computational burden on users in this scheme is too heavy and not very practical.

2.3. Attribute and Policy hiding. As the application of CP-ABE for medical data sharing becomes more widespread, related security issues arise because most CP-ABE schemes embed attribute values into ciphertexts, and attackers can easily infer private attributes from ciphertexts, leading to the exposure of patients' privacy. Lai et al. [33] proposed a method to hide access policy by inner product encryption, which achieves complete policy hiding and is proven to be completely secure. However, the scheme applies to small universes, and in short, the key becomes larger with the increase in the number of attributes, making it less scalable and unsuitable to be combined with blockchain due to its high scalability requirement. Hur [34] proposed a hidden access structure applied to smart grids in which the access policy can be represented by an arbitrary access formula. However, in this scheme, the length of the private key possessed by the user is too long, greatly increasing the storage burden of the user, and there is no security proof to demonstrate the security of this scheme. Gao et al. [17] proposed a completely secure blockchain-based policy-hiding scheme called TrustAccess, which resolves the problem of centralization and a small universe. Nonetheless, in this scheme, the ciphertext is stored locally by the data owner, i.e., the patient, who is also responsible for generating the key. When applied to a medical data-sharing system, it is impractical due to the huge amount of medical data, which cannot be handled by ordinary devices such as the patient's cell phone. Michalevsky and Joye [35] proposed an ABE scheme for hiding attributes, which supports conjunctions, disjunctions, and threshold policies. However, in this scheme, although the entire set of attributes is hidden, the attributes controlled by the attribute authority are still displayed.

3. Preparations

First, we present the symbols used in this paper in Table 1.

3.1. Blockchain. The blockchain originated from the Bitcoin system proposed by Satoshi Nakamoto in 2008 [36]. The consortium blockchain requires permission for nodes to join the network and needs to be jointly maintained by all nodes, with some of the nodes in the consortium blockchain assumed to be trusted [37, 38]. The scheme used in this study involves the consortium blockchain. In terms of the structure of a blockchain, each data block consists of a block header and a block body. To ensure data integrity and tamper resistance, each block header contains the cryptographic hash of the previous block, while the block body contains detailed information about the transactions. An important component in the blockchain is the consensus algorithm, in blockchain, since nodes are untrustworthy to each other, when nodes update data between them, a consensus algorithm is needed to reach consensus to update data [38, 39]. Most of the current coalition chains use the PBFT algorithm, which is based on the Byzantine general problem and has the advantages of high consistency of consensus results and fast confirmation [40]. The consensus algorithm used in this scheme is the PBFT algorithm. This algorithm is based on the Byzantine general's problem and has the advantages of high consensus result consistency and fast confirmation.

Table 1: Notations in this paper.

Notation	Description
G/G_T	The cyclic multiplicative groups
A	Access policy
Att	User's attribute set
Γ	The tree-structured access policy
$SymKey$	The symmetric encryption key
λ	The security parameter
PK	The public key
MSK	The master secret key
CT_m	The ciphertext of medical data
CT	The ciphertext of the symmetric key
$Txst$	Information transaction
$Txac$	Access transaction
$\vec{x}$	The vector generated by the attribute set
$\vec{D}$	Attribute hiding vector

3.2. Composite Order Bilinear Groups. The use of composite order bilinear groups in algorithms such as encryption in this scheme was first introduced by Boneh et al. [41].

Definition 1 (Composite Order Bilinear Groups). Let G and G_T be multiplicative cyclic groups of order $n = pqr$, where p, q, r are distinct prime numbers. $\widehat{e} : G \times G_T$ is a mapping, where G_p, G_q, G_r to denote the subgroups of G with order p, q, and r, respectively, can be obtained as $G = G_p \times G_q \times G_r$, and for any $g_p \in G_p, g_q \in G_q$, have $\widehat{e}(gp\ ,\ g_q) = 1$ with the following properties:

(1) Bilinearity: $\forall u, v \in G, \forall a, b \in Z_N, \widehat{e}(u^a, v^b) = \widehat{e}(u,\ v)^{ab}$.
(2) Nondegeneracy: $\exists g \in G$, such that $\widehat{e}(g, g)$ has ordered N in G_T.
(3) Computability: $\forall u, v \in G$, there exists a polynomial-time algorithm associated with a given safety constant λ that can efficiently compute $\widehat{e}(u, v)$.

3.3. Attribute Sets and Access Policies

Definition 2 (Attribute Sets and Access Policies [17, 36]). First associate each attribute with a unique element Z_N, which is implemented with the $\{0,\ 1\}^* \longrightarrow Z_N$ collision-resistant hash function H. Let the matrix $V = (V_1, \ldots, V_i, \ldots, V_n)$ of $n \times l$ be the possible attributes, where vectors $V_i = (k_{i,1}, \ldots, k_{i,j}, \ldots, k_{i,l}), k_{i,j} \in Z_N$. V_i is the possible value of the attribute in the ith attribute category, so when the user's attribute set is $Att = (w_1, \ldots, w_i, \ldots, w_n)$, it can be expressed as $Att = (k_{1,j_1}, k_{2,j_2}, \ldots, k_{i,j_i}, \ldots, k_{n,j_n})$, where $w_i \in V_i, j_i \in \{1, \ldots, l\}$. If there is an access policy $A = (W_1, \ldots, W_n)$, where $W_i \in V_i$, the set of attributes matches the access policy, then when and only when $k_{i,j_i} \in W_i$, $1 \leq i \leq n$.

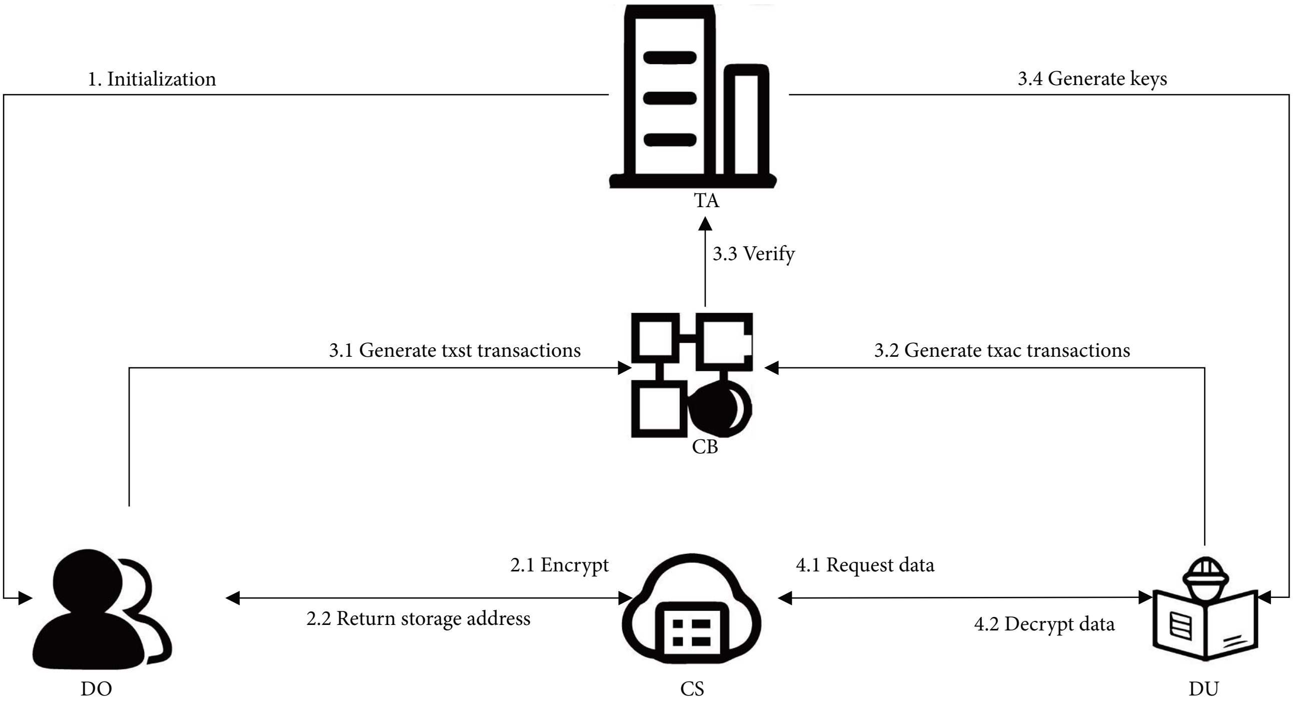

Figure 1: Flowchart.

3.4. Inner Product Predicate. The access policy Γ is represented as a tree structure. The following describes how the access policy is represented as an equation and how the set of attributes is represented as a vector. It is first known that the set of attributes is representable as a vector of $(d+1)^t$ elements, where t denotes the class of the attribute and d denotes the number of attribute values [17, 42].

Define that predicates I_1 and I_2 can be encoded as polynomials if $x_1 = I_1, x_2 = I_2$.

$$p(x_1, x_2) = (x_1 - I_1) + h \cdot (x_2 - I_2), h \in Z_N. \quad (1)$$

Defining the predicate I_1 or I_2 can be encoded as a polynomial, if $x = I_1$ or $x = I_2$.

$$p(x) = (x - I_1) \cdot (x - I_2). \quad (2)$$

Here is an example to illustrate how to represent the access policy by a polynomial and the set of attributes by vector. Suppose there are $t = 3$ classes of attributes in a healthcare data-sharing system, section, position, and title, respectively, $d = 1$, so the access structure is as follows:

$\Gamma = (\text{department: Pediatrics OR Position: physician})\text{AND}$ $(\text{positional titles: chief physician})$. Then, the access structure can be expressed by the following polynomial:

$$\begin{aligned} p(x_1, x_2) &= (x_1 - I_{pe}) \cdot (x_1 - I_{ph}) + h \cdot (x_2 - I_{ch}) \\ &= x_1 \cdot x_1 - h \cdot x_2 - (I_{pe} + I_{ph}) \cdot x_1 + I_{pe} \cdot I_{ph} - h \cdot I_{ch}, \end{aligned} \quad (3)$$

when the user has an attribute set of

$Att = (\text{department: Pediatrics, Position: physician,}$ $\text{positional titles: chief physician})$. Then, the set of attributes of the user can be represented by the following vector:

$$\vec{x} = (I_{pe} \cdot I_{ph} \cdot I_{ch}, I_{pe} \cdot I_{ph}, I_{ph} \cdot I_{ch}, I_{pe} \cdot I_{ch}, I_{pe}, I_{ph}, I_{ch}, 1). \quad (4)$$

3.5. System Framework

3.5.1. System Model. As shown in Figure 1, in the HA-Med system, there are five entities involved, which are the data owner (DO), data user (DU), blockchain (CB), trusted authority (TA), and cloud system (CS).

(1) Data Owner (DO). The DO is the patient, the entity that generates the medical data. The DO is responsible for developing the access policy, as well as encrypting the data. All ciphertexts are sent to the CS. To achieve secure access control, the DO sends the ciphertext address and access structure polynomial to the CB by storing the transaction.

(2) Data User (DU). The DU is a hospital, medical research center, etc. The DU uses a private identity key to send the attribute set of a hidden access structure to the CB and TA for verification. If it meets the access policy, then the DU can obtain the key and decrypt the medical data.

(3) Blockchain (CB). The consortium blockchain selected in this scheme is a peer-to-peer network, a distributed platform for recording storage and access transactions, consisting of DO, DU, and a selected trusted institution TA. Due to the immutability and data recording characteristics of the blockchain, medical data can be securely shared and collaborated through the blockchain. Additionally, the blockchain

enables secure and transparent access control, thereby ensuring the security of medical data. Moreover, the blockchain can also achieve traceability of medical data, allowing the source and usage of data to be traced and verified.

(4) Trusted Authority (TA). Trusted authorities (TA) are, for example, government agencies and trusted third parties selected by the blockchain consensus algorithm. They generate public parameters for the system and perform off-chain verification. If the hidden access policy and attributes are matched successfully, the key is generated for the DU, and the TA does not know the access policy and attributes during the verification process.

(5) Cloud Storage System (CS). The DO stores encrypted medical data and an encrypted symmetric key on the cloud. When the DU has the decryption key, the cloud returns the data to the patient's address for decryption.

3.5.2. Overview of the Program.

(1) Initialization Phase. This phase initializes the parameters in the system, such as the complex order bilinear group, etc. DO and DU generate the public and private keys for signing transactions in this phase.

(2) Encryption Phase. First DO decides its access structure based on a set of attributes and then encrypts the medical data using a symmetric key $SymKey$ to obtain CT_m, next encrypts the symmetric key with the encryption algorithm to get the ciphertext CT, upload CT_m and CT to the cloud storage, and the cloud returns to the DO storage address.

(3) Verification Stage.

1. DO register transactions that send encrypted access policies to the blockchain.
2. All the DUs who want to access the medical data send the stored transactions with encrypted attributes to the blockchain.
3. The TA receives both transactions and gets the encrypted access policy and attributes for off-chain matching.
4. TA generates a decryption key for DU.

(4) Decryption and Access Phase.

1. When DU gets the decryption key, it will request the ciphertext from CS.
2. CS returns to DU ciphertext, and DU decrypts the symmetric key, in which the symmetric key is used to decrypt the medical data, and then access the medical data.

The exact process is described in detail in Section 5.

3.5.3. Algorithms Overview.

(1) Initialization. $Setup(1^{\lambda}) \longrightarrow (PK, MSK)$. This phase initializes the parameters in the system, and the trusted authority TA runs the algorithm to generate the public key and the master key.

(2) Encryption. DO run the encryption algorithm to generate the encrypted ciphertext CT. To achieve the hiding of the access policy, the access structure is not embedded in the ciphertext, and it is decrypted only for users who conform to the access policy.

(3) Key Generation. $KeyGen(PK, MSK) \longrightarrow DecKUID$. When the TA verifies that the DU attributes match the DO access policy, run the algorithm and enter the public key PK and the master key MSK, generate a key $DecKUID$ for the DU that can decrypt the ciphertext CT and issue it to the DU.

(4) *Decryption.* $Dec(PK, CT, DecKUID) \longrightarrow SymKey$. When DU gets the decryption key, it will request the ciphertext from CS, CS returns the ciphertext to DU, and DU decrypts it.

3.5.4. Security Model. Since this scheme uses a consortium blockchain, it is considered that each node is honest but also curious [43], and the nodes, although they will follow the protocol of this scheme and will also try to find out as much secret data as possible [17]. In the following, the security model will be given, described as a security game between a challenger and an adversary, based on [42], the security game is described as follows:

(1) Setup. The challenger runs an algorithm $Setup(1^{\lambda})$ to obtain the public key PK and the master key MSK. The public key PK is given to the adversary, and the master key MSK is kept by itself.

(2) Inquiry Phase 1. The adversary adaptive query queries the challenger for the key and in response, the challenger runs the algorithm $KeyGen(PK, MSK)$ to generate the key $DecKUID$ to the adversary.

(3) Challenge. The adversary submits two messages $SymKey_0, SymKey_1$ and two restricted access structures Γ_0, Γ_1. These strategies cannot be satisfied by any of the attributes set being queried. The challenger chooses a random bit $\beta \in \{0,\ 1\}$ and runs $CT^* \longleftarrow Enc(PK, SymKey_{\beta}, \Gamma_{\beta})$ and sends CT^* as a challenge cipher to the adversary.

(4) Query Phase 2. The adversary continues to adaptively query the challenger for the key and adds the restriction that none of these attributes satisfy the Γ_0, Γ_1 restrictions.

(5) Guess. The opponent outputs a guess for $\beta, \beta' \in 0, 1$. If $\beta = \beta'$, wins the game.

In this game, the opponent's advantage is defined as $P = Pr[\beta = \beta'] - \frac{1}{2}$, where the probability is occupied by the random bits used by the challenger and the opponent.

Definition 3. If the polynomial-time adversary has at most a negligible advantage P in this security game, then the proposed CP-ABE with hidden strategies and properties is completely secure.

3.6. Detailed Solutions. In this section, the detailed construction of the HA-Med program is described.

3.6.1. Initialization Phase. Taking the safety parameter λ as input and running the group generator $\boldsymbol{G}\ (1^{\lambda})$ gives$(p, q, r, G, G_T, \widehat{e}), G = G_p \times G_q \times G_r, G$ and G_T are cyclic groups of order $N = pqr$. $Setup(1^{\lambda})$ algorithm run by TA, It selects generators g_p and g_r of G_p and G_r, respectively. Then, randomly selects $a, w \in Z_N$, and chooses and $R_1 \in G_r$ uniformly at random to obtain the public key.

$$PK = \left(A_0 = g_p \cdot R_0, A_1 = g_p^a \cdot R_1, g_r, Y = \widehat{e}\left(g_p, g_p\right)^w\right). \tag{5}$$

The master key is as follows:

$$MSK = \left(g_p, a, w\right). \tag{6}$$

3.6.2. Encryption Phase. In this phase, the DO decides on a set of access policies Γ. $\Gamma = (W_1, \cdots, W_i, \cdots, W_n)$, which $W_i \subseteq V_i$. First, DO encrypts the medical data with the symmetric key *SymKey* to get ciphertext CT_m. $Enc(PK, SymKey, \Gamma)$ the algorithm is run by the DO, which first randomly selects $s \in Z_N$, $R_0' \in G_r$. Then, choose $s_{i,j} \in Z_N$, $R_{i,j}' \in G_r$ randomly and calculate $\tilde{C} = SymKey \cdot Y^s$, $C_0 = A_0^s \cdot R_0'$, when $1 \leq i \leq n$, $1 \leq j \leq l$ then calculate the following:

$$C_{i,j} = \begin{cases} A_1^s \cdot R_{i,j}^{'}, k_{i,j} \in W_i \\ A_1^{s^{i,j}} \cdot R_{i,j}^{'}, \text{otherwise} \end{cases}. \tag{7}$$

The final generation of ciphertext $CT = (\tilde{C}, C_0, \{C_{i,j}\}_{1 \leq i \leq n, 1 \leq j \leq l})$. DO uploads CT_m and CT to the cloud storage and the cloud returns to the DO storage address.

3.6.3. Verification Phase. This phase is divided into four parts: the registration of transactions containing hidden access policies and attributes for DU and DO, the verification of DU compliance with DO's access policies, and key generation by TA.

(1) Generating Txst Storage Transactions. First, DO generates the transaction as follows:

$$Txst = \{S, \text{Sign}_{DO}, Px, \text{code}, CT_{\text{Adress}}\}, \tag{8}$$

where S is the identification of the transaction; $Sign_{DO}$ is the digital signature generated by the DO's private key registered in the CB; Px is a polynomial expression of the access structure; *code* is the full check digit of the ciphertext, used to ensure the integrity of ciphertext; CT_{Adress} is the address where the ciphertext is stored in the cloud.

(2) Generating Txac Access Transactions. When DU wants to request access to medical data, it first multiplies the elements in the vector $\vec{x}$ generated by the attribute set by the same factor R_3, where $R_3 \in G_r$, get $\vec{D}$, For example, when $\vec{x} = (I_{pe}I_{ph}I_{ch}, I_{pe}I_{ph}, I_{ph}I_{ch}, I_{pe}I_{ch}, I_{pe}, I_{ph}, I_{ch}, 1)$ obtain $\vec{D} = (I_{pe}I_{ph}I_{ch} \cdot R_3, I_{pe}I_{ph} \cdot R_3, I_{ph}I_{ch} \cdot R_3, I_{pe}I_{ch} \cdot R_3, I_{pe} \cdot R_3, I_{ph} \cdot R_3, I_{ch} \cdot R_3, R_3)$ generate the transaction as follows:

$$Txac = \left\{A, \text{Sign}_{DU}, \vec{D}, CT_{\text{Adress}}\right\}, \tag{9}$$

where A is the transaction identifier; $Sign_{DU}$ is the digital signature generated by DU's private key registered in CB; $\vec{D}$ is the attribute hiding vector; CT_{Adress} is the address of the medical data that DU requests to access.

(3) Verification. T*xst* and *Txac* are broadcast to the CB, respectively, if the attributes of DU satisfy the access structure of DO, then it is known that the elements in the DU attribute vector are solutions of the polynomial of the access structure of DO, then TA performs the following operations after receiving.

For example $Px = x_1^2 - h \cdot x_2 - (I_{pe} + I_{ph}) \cdot x_1 + I_{pe} \cdot I_{ph} - h \cdot I_{ch}$, set $Px = 0$ and perform the following operation:

$$e(R_3, R_3)^{Px} = 1, \tag{10}$$

$$e(R_3, R_3)^{x_1^2 - h \cdot x_2 - \left(I_{pe} + I_{ph}\right) \cdot x_1 + I_{pe} \cdot I_{ph} - h \cdot I_{ch}} = 1, \tag{11}$$

$$\begin{aligned} & e(R_3, R_3)^{x_1^2} \cdot e(R_3, R_3)^{-\mathrm{h}x_2} \cdot e(R_3, R_3)^{-I_{pe}x_1} \cdot e(R_3, R_3)^{-I_{ph}x_1} \\ & \quad \cdot e(R_3, R_3)^{I_{pe}I_{ph}} \cdot e(R_3, R_3)^{-hI_{ch}} = 1 \\ & e(x_1R_3, x_1R_3) \cdot e(-hR_3, x_2R_3) \cdot e\left(-I_{pe}R_3, x_1R_3\right) \\ & \quad \cdot e\left(-I_{ph}R_3, \mathrm{x}_1R_3\right) \cdot e\left(I_{pe}R_3, I_{ph}R_3\right) \cdot e(-hR_3, I_{ch}R_3) = 1. \end{aligned} \tag{12}$$

Then, TA verifies whether $\vec{D}$ can make the equation hold.

(4) Key Generation. When the TA verifies that the DU matches the DO access structure, a key is generated for the DU and the $KeyGen(PK, MSK) \longrightarrow DecKUID$ algorithm is run. Randomly choose $ti \in Z_N$, where $i = 1, 2, \ldots, n$, and set $t = \sum_{i=1}^{n} t_i$, then calculate the following:

$$D_0 = g_p^{w-t}, \ D_i = g_p^{t_i/a}. \tag{13}$$

The key is obtained as follows:

$$DecKUID = \left(D_0, \{D_i\}_{1 \leq i \leq n}\right). \tag{14}$$

(5) *Decryption Phase*. This stage is the DU decryption stage; when the DU conforms to the access policy to get the access key, the DU requests medical data from the CS; at this time, the CS will return to DU CT_m and CT. First DU runs the $\mathrm{Dec}(PK, CT, DecKUID) \longrightarrow SymKey$ algorithm to get the symmetric key *SymKey*.

$$\begin{aligned} SymKey &= \frac{\widetilde{C}}{\widehat{e}(C_0, D_0) \cdot \prod_{i=1}^{n} \widehat{e}\left(C_{i,j_i}, D_i\right)} \\ &= \frac{SymKey \cdot Y^s}{\widehat{e}\left(A_0^s \cdot R_0', g_p^{w-t}\right) \cdot \prod_{i=1}^{n} \widehat{e}\left(A_1^s \cdot R_{i,j_i}', g_p^{t_i/a}\right)} \\ &= \frac{SymKey \cdot \widehat{e}\left(g_p, g_p\right)^{ws}}{\widehat{e}\left(g_p^s, g_p^{w-t}\right) \cdot \prod_{i=1}^{n} \widehat{e}\left(\left(g_p^a\right)^s, g_p^{t_i/a}\right)} \\ &= \frac{SymKey \cdot \widehat{e}\left(g_p, g_p\right)^{ws}}{\widehat{e}\left(g_p^s, g_p^{w-t}\right) \cdot \prod_{i=1}^{n} \widehat{e}\left(g_p^s, g_p^{t_i}\right)} \\ &= \frac{SymKey \cdot \widehat{e}\left(g_p, g_p\right)^{ws}}{\widehat{e}\left(g_p^s, g_p^w\right)}. \end{aligned} \tag{15}$$

After getting the symmetric key, decrypt the medical data with the symmetric key *SymKey*.

3.7. Security Analysis

3.7.1. Privacy. The current access control scheme, based on the combination of attribute encryption and blockchain, directly stores the attributes and access policies on the blockchain, leading to potential privacy leakage due to the transparency of the blockchain. In HA-Med, access policies and attributes are initially hidden through polynomials and vectors, preventing eavesdroppers from accessing them. Additionally, although third-party verification is involved, they only receive hidden access policies and attributes during verification and cannot obtain the actual data. They solely perform calculations, and sensitive data such as attributes and access structures are not exposed. Finally, the data transmitted to the blockchain is only the hidden data, thus eliminating the risk of exposure.

3.7.2. Integrity. In this scheme, the TA can get the complete data to prevent the tampering of the data address on the chain. The complete ciphertext checksum is included in the transaction, so the integrity of the ciphertext can be checked by the ciphertext checksum at any time.

3.7.3. Traceability. Because this solution introduces blockchain, which is traceable, any access by DU is recorded as immutable stored transactions for traceability and accountability. In addition, DO can know all access records of DU, including who accessed the data and what data were accessed.

3.7.4. Security Analysis of CP-ABE with Hidden Attributes and Access Structures. The security proof of this scheme is based on the following several complexity assumptions, where Assumptions 1, 2, and 3 are the same as those in [17, 33, 44, 45], and Assumption 4 is the same as those in [17, 33, 44, 46], and these assumptions are also used to prove security in the above paper, as described below:

Assumption 1. *Given a group generator* $\mathbf{G}$, *the following distribution is then defined.*

$(N = pqr, G, G_T, \widehat{e}) \longleftarrow \mathbf{G}$ $g_p \overset{R}{\longleftarrow} G_p$, $g_r \overset{R}{\longleftarrow} G_r$,

$D = (N, G, G_T, \widehat{e}, g_p, g_r)$, $T_1 \overset{R}{\longleftarrow} G_{\mathrm{p}} \times G_{\mathrm{q}}$, $T_2 \overset{R}{\longleftarrow} G_p$

The advantage of algorithm A in breaking this assumption is defined as follows:

$$Adv1_A = |Pr[A(D, T_1) = 1] - Pr[A(D, T_2) = 1]|. \tag{16}$$

Definition 4. If $Adv1_A$ is negligible for any probabilistic time polynomial time algorithm A, then G satisfies Assumption 1.

Assumption 2. *Given a group generator* $\mathbf{G}$, *the following distribution is then defined.*

$(N = pqr, G, G_T, \widehat{e}) \longleftarrow \mathbf{G}$, g_p, $X_1, Y_1 \overset{R}{\longleftarrow} G_p$, X_2, $Y_2 \overset{R}{\longleftarrow} G_q$, $g_r \overset{R}{\longleftarrow} G_r$, $D = (N, G, G_T, \widehat{e}, g_p, X_1X_2, Y_1Y_2, g_r)$, $T_1 \overset{R}{\longleftarrow} G_P \times G_q$, $T_2 \overset{R}{\longleftarrow} G_p$。

The advantage of algorithm A in breaking this assumption is defined as follows:

$$Adv2_A = |Pr[A(D, T_1) = 1] - Pr[A(D, T_2) = 1]|. \tag{17}$$

Definition 5. If $Adv2_A$ is negligible for any probabilistic time polynomial time algorithm A, then G satisfies Assumption 2.

Assumption 3. *Given a group generator* $\mathbf{G}$, *the following distribution is then defined.*

$(N = pqr, G, G_T, \widehat{e}) \longleftarrow \mathbf{G}$, $w, s \in Z_N$, g_p, $Z_1 \overset{R}{\longleftarrow} G_p$, X_2, Y_2, $Z_2 \overset{R}{\longleftarrow} G_q$, $g_r \overset{R}{\longleftarrow} G_r$,

$D = (N, G, G_T, \widehat{e}, g_p, g_p^w X_2, g_p^s Y_2, Z_1Z_2, g_r)$, $T_1 \overset{R}{\longleftarrow} \widehat{e}^{(g_p, g_p)ws}$, $T_2 \overset{R}{\longleftarrow} G_T$。

The advantage of algorithm A in breaking this assumption is defined as follows:

$$Adv3_A = |Pr[A(D, T_1) = 1] - Pr[A(D, T_2) = 1]|. \tag{18}$$

Definition 6. If $Adv3_A$ is negligible for any probabilistic time polynomial time algorithm A, then G satisfies Assumption 3.

Assumption 4. *Given a group generator G, the following distribution is then defined.*

$(N = pqr, G, G_T, \widehat{e}) \longleftarrow \mathbf{G}$, $a \in Z_N$, $g_p \overset{R}{\longleftarrow} G_p$, g_q, Q_1, $Q \overset{R}{\longleftarrow} G_q$, g_r, $R_0, R_1, R \overset{R}{\longleftarrow} G_r$, $D = (N, G, G_T, \widehat{e}, g_pR_0, g_p^aR_1, g_pQ_1, g_q, g_r)$, $T_1 = g_p^aQR$, $T_2 \overset{R}{\longleftarrow} G_T$。

The advantage of algorithm A in breaking this assumption is defined as follows:

$$Adv4_A = |Pr[A(D, T_1) = 1] - Pr[A(D, T_2) = 1]|. \tag{19}$$

Definition 7. If $Adv4_A$ is negligible for any probabilistic time polynomial time algorithm A, then G satisfies Assumption 4.

Table 2: Symbols used in the theoretical analysis.

Notation	Description
E_t	Exponentiation in G_t
E	Exponentiation in G
N	Number of attributes
Sym	Symmetric encryption and decryption operation
$N2$	Number of positive attributes
$N3$	Number of negative attributes
W	Number of wildcards
P	Pairing operation

Table 3: Comparison with related work.

Scheme	MedSBA [12]	BC-SABE [29]	Hidden [47]	RS-HABE [28]	Ours
Expressiveness	AND	LSSS	AND	LSSS	AND
Hidden strategies	×	×	√	×	√
Auditability	√	√	×	×	√
Forward secrecy	√	×	×	√	√
Properties revocation	√	√	×	√	√

Theorem 1. *The proposed CP-ABE with hidden access structure and policy are completely secure if* $\mathbf{G}$ *satisfies Assumptions 1, 2, 3, and 4.*

Proof. The proof of security is given in the appendix. □

3.8. Analysis of Performance. In this section, separate theoretical and experimental analyses are performed to evaluate the performance of HA-Med. Some of the relevant symbols used are shown in Table 2.

3.8.1. Theoretical Analysis. In Table 3, this scheme is compared with some related schemes [12, 28, 29, 47] in five aspects: access policy, whether it supports policy hiding, auditability, whether it has forward secrecy, and attribute revocation, respectively. In Table 2, it can be seen that [12], although the combination with blockchain achieves a trusted access process, also due to the transparency of blockchain, the access policy and attributes are sent directly to the blockchain, which can cause privacy leakage to users and data owners [29] proposed an access control scheme that combines with blockchain and distributes keys through consensus nodes, which solves the problem of third parties but does not have forward confidentiality also due to the transparency of blockchain, no policy hiding is performed, which can cause privacy leakage of access policies and user attributes [47], achieves attribute and access policy hiding, but does not have forward confidentiality and attribute revocation [28], achieved secure sharing of attribute revocation EHRs by combining them with public clouds. However, the same privacy protection in this aspect of attributes is not achieved. The proposed HA-Med scheme improves the schemes of Phuong et al. [47] and Gao et al. [17] to achieve a blockchain-based attribute-hiding medical data-sharing scheme.

As for the computational cost of the HA-Med scheme, in terms of encryption, the symmetric encryption algorithm is first performed once by the DO, and then $N+2$ powers are taken in G. In [29], one symmetric encryption algorithm is performed followed by taking $4\text{N}+2$ powers and one power in G and G_T, respectively. For key generation, only $N+1$ powers in G are needed. In [47, 48], we also need to take more powers in G, respectively; in decryption, DU first performs $N+1$ pairing operations and then decrypts the ciphertext by performing one symmetric decryption. In [29, 47, 48], the pairing operations of constant order are also required, respectively. In Table 4, this scheme is compared with [29, 47, 48], and it can be seen that the computational costs are all within a reasonable range.

In conclusion, the above theoretical analysis shows that HA-Med achieves better security, exhibits better functionality, protects patient and user privacy, and enables easy access to medical data without any increase in computational cost compared to other solutions.

3.8.2. Experimental Analysis. The consensus algorithm has a significant impact on the efficiency of the blockchain. In HA-Med, we have adopted the PBFT consensus algorithm to improve efficiency. Additionally, in our system, we do not store the ciphertext on the blockchain; instead, we store the ciphertext address on the blockchain, which also enhances the scalability of the blockchain. Given that the focus of this scheme is on the security and performance of ABE, the main emphasis is on the efficiency of ABE.

The main implementation of this solution utilizes the JPBC library in Java, which was carried out on a Windows 10 laptop with a 2.70 GHz Intel (R) Core (TM) i5-7200U CPU and 8 GB RAM. Comparative experiments were conducted on ABE algorithms, specifically comparing the encryption, key generation, and decryption phases with the schemes proposed by Lewko and Waters [49] and Lai et al. [33]. HA-Med introduces attribute-hiding functionality compared to the scheme by Lewko and Waters [49], and it satisfies the large universe access requirement compared to the scheme by Lai et al. [33], thereby enhancing scalability. The experimental results are presented in Figures 2–4. As depicted in the figures, the encryption time, key generation time, and decryption time all increase with the number of attributes. HA-Med demonstrates shorter processing times compared to the schemes proposed by Lewko and Waters [49] and Lai et al. [33]. Overall, it is evident that this solution achieves complete hiding of access policies and attributes within a reasonable CP-ABE algorithm time frame, ensuring the security of data owners and users.

4. Conclusion

In this paper, we propose a healthcare data access control scheme that achieves fine-grained access control while integrating with blockchain for improved scalability. We introduce a verification method to address the privacy leakage problem of user attributes and access policies in the current CP-ABE scheme, achieving complete policy hiding, forward confidentiality, and attribute revocation. Additionally, traceability is achieved by registering

Table 4: Comparison of computational performance.

Scheme	Encryption	Key generation	Decryption
Melissa chase [48]	$E_t+(N+1)E$	$9NE$	$(4n+2)P$
Hidden [47]	$E_t+(2+6N)E$	$(2wN2+2wN3+4w)E$	$(4w+2)P$
BC-SABE [29]	$Sym+(4N+2)E+E_t$	–	User: E_t+Sym Cloud: $NE_t+(3N+2)P$
Ours	$Sym+(N+2)E$	$(N+1)E$	$P(N+1)+Sym$

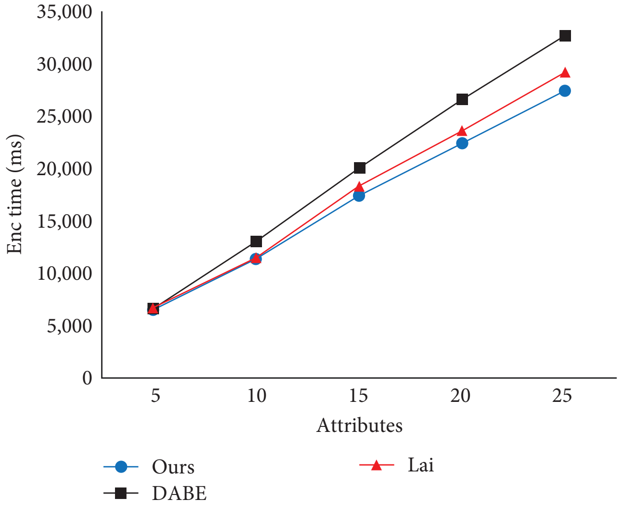

Figure 2: Encryption time.

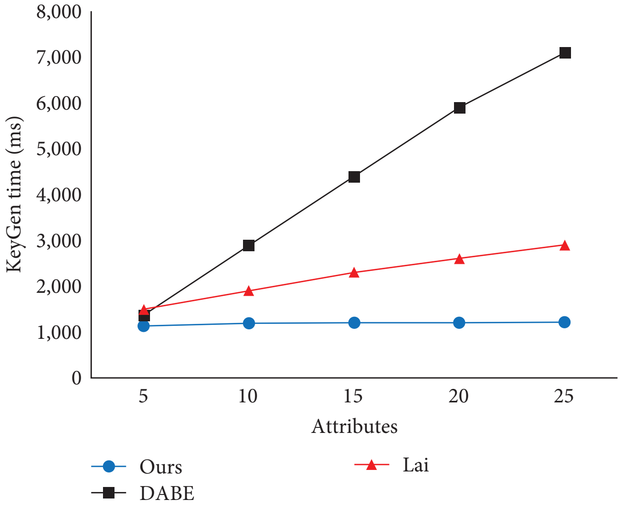

Figure 3: Key generation time.

transactions on the blockchain to access medical data. Considering the large size of realistic medical data, storing the data in the cloud instead of on the user side reduces the storage overhead for the user. Finally, theoretical and experimental analysis demonstrates the feasibility of this scheme, showing better security and higher scalability than existing schemes. However, HA-Med still has shortcomings in the efficiency of the verification method, and future work will primarily focus on improving the efficiency of the verification method.

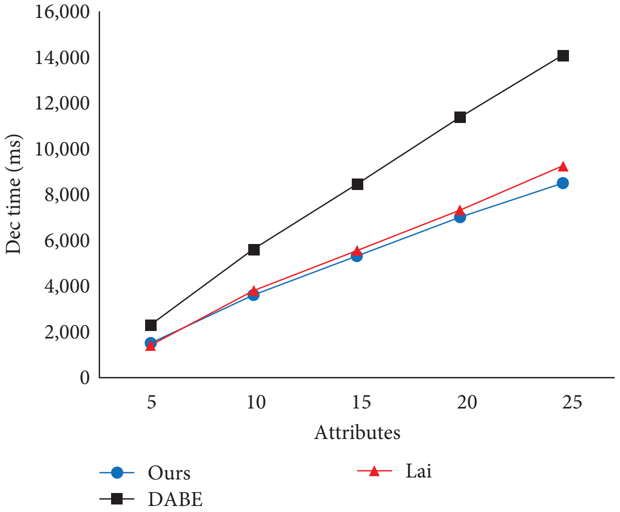

Figure 4: Decryption time.

Appendix

Security Proof CP-ABE on Hiding Strategy

Proof. To prove the security of CP-ABE for our proposed hiding strategy, we introduce the concept of dual-system encryption introduced by Waters [50], where first we define two additional structures, a semi-functional ciphertext and a semi-functional key. These two structures will not be used in the actual system but will be used in our proof.

Semi-functional ciphertext. Let g_q denote the generating element of the subgroup G_q. Create a semi-functional ciphertext as follows: first, generate a normal ciphertext using the encryption algorithm *Enc* as follows: □

$$CT' = \left(\widetilde{C}', C_0', \left\{C_{i,j}\right\}'_{1\le i\le n, 1\le j\le l}\right). \tag{A.1}$$

Then, when $1\le i\le n, 1\le j\le l$, we randomly choose x_0, $x_{i,j}\in Z_N$, the final semi-functional ciphertext is as follows:

$$CT = \left(\widetilde{C}=\widetilde{C}', C_0 = C_0'\cdot g_q^{x_0}, \left\{C_{i,j} = C'_{i,j}\cdot g_q^{x_{i,j}}\right\}_{1\le i\le n, 1\le j\le l}\right). \tag{A.2}$$

Semi-Functional Keys. Let g_q denote the generating element of the subgroup G_q. Create a semi-functional key as follows, first generating a common key using the key generation algorithm *KeyGen* as follows:

$$\mathrm{DecKUID} = \left(D'_0, \{D'_i\}_{1 \le i \le n}\right). \tag{A.3}$$

Then, when $1 \le i \le n$, we randomly choose the indices y_0, $y_i \in Z_N$, and the final semi-functional key as follows:

$$\mathrm{DecKUID} = \left(D_0 = D'_0 \cdot g_q^{y_0}, \{D_i = D'_i \cdot g_q^{y_i}\}_{1 \le i \le n}\right). \tag{A.4}$$

We will use the following series of games to prove security by mixed arguments. The first game, $Game_{real}$, is a truly secure game, where both the ciphertext and the key are secure. In $Game_1$ (or $Game_{2,0}$), the key is normal and the ciphertext is semi-functional. In $Game_{2,\mathrm{k}}$, the ciphertext is semi-functional, the first k keys are semi-functional, and the rest are normal. In $Game_3$, all ciphertexts and keys are semi-functional, but the ciphertext is a semi-functional encryption of a random message and not a message provided by the adversary. In $Game_3$, the game is the same as $Game_3$, except that the ciphertext is independent of what the adversary provides $\varGamma_1, \varGamma_2$, neither of the adversary's advantages in $Game_3$ can be greater than 0.

Our proof requires the following four lemmas, which are formally described below:

Lemma A.1. *Suppose* G *satisfies Assumption 1, then* $Game_{real}$ *and* $Game_1$ *are indistinguishable.*

Proof. Assuming that algorithm A can distinguish between $Game_{real}$ and $Game_1$, then we construct an algorithm B that has a nonnegligible advantage for breaking Assumption 1. B is given g_p, g_r, T, and A simulates $Game_{real}$ and $Game_1$. □

B random selection $a, a_1, a_2, w \in Z_N$, setting $R_0 = g_r^{a_1}$, $R_1 = g_r^{a_2}$, $A_0 = g_p \cdot R_0$, $A_1 = g_p^a \cdot R_1$, and sends the public key to A.

$$PK = \left(A_0, A_1, g_r, Y = \widehat{e}(g_p, g_p)^w\right). \tag{A.5}$$

B can run the key generation algorithm to generate a normal key in response to A's key request. A sends B two messages of equal length $SymKey_1, SymKey_2$ and two access policies $\varGamma_1, \varGamma_2$. B randomly selects $\beta \in \{0, 1\}$ and performs the following actions:

(1) B random selection $s \in Z_N, R'_0 \in G_r$, $s_{i,j} \in Z_N$, and $R'_{i,j} \in G_r$.

(2) B calculate $\tilde{C} = SymKey_\beta \cdot \widehat{e}(g_p^w, T), C_0 = T \cdot R_0^s \cdot R'_0$, and when $1 \le i \le n$, $1 \le j \le l$, and $r_{i,j} = s_{i,j}/as$ calculate the following:

$$C_{i,j} = \begin{cases} T^a \cdot R_1^s \cdot R'_{i,j}, v_{i,j} \in W_i; \\ T^{a \cdot r_{i,j}} \cdot R_1^{s_{i,j}} \cdot R'_{i,j}, \text{otherwise} \end{cases}. \tag{A.6}$$

(3) B set the challenge cipher $CT = (\tilde{C}, C_0, \{C_{i,j}\}_{1 \le i \le n, 1 \le j \le l})$ at this time, and send this to A.

If $T \xleftarrow{R} G_p \times G_q$, then let $T = g_p^s g_q^{x_0}, \tilde{C} = SymKey_\beta \cdot \widehat{e}(g_p, g_p)^{ws}$, $C_0 = g_p^s g_q^{x_0} \cdot R_0^s \cdot R'_0$, and when $1 \le i \le n$, $1 \le j \le l$

$$x_{i,j} = \begin{cases} ax_0, \ v_{i,j} \in W_i \\ ax_0 r_{i,j}, \text{otherwise} \end{cases}, \tag{A.7}$$

calculate

$$C_{i,j} = \begin{cases} g_p^{as} g_q^{x_{i,j}} \cdot R_1^s \cdot R'_{i,j}, v_{i,j} \in W_i \\ g_p^{as_{i,j}} g_q^{x_{i,j}} \cdot R_1^{s_{i,j}} \cdot R'_{i,j}, \text{otherwise} \end{cases}. \tag{A.8}$$

Therefore, the ciphertext is semi-functional, and B simulates $Game_1$.

If $T \xleftarrow{R} G_p$, the ciphertext is the normal ciphertext, and B simulates $Game_{real}$. Finally, B distinguishes the possibility of T by the output of A.

Lemma A.2. *Suppose* **G** *satisfies Assumption 2, then* $Game_{2,\mathrm{k}-1}$ *and* $Game_{2,\mathrm{k}}$ *are indistinguishable.*

Proof. Suppose an algorithm A can distinguish between $Game_{2,\mathrm{k}-1}$ and $Game_{2,\mathrm{k}}$, then we construct an algorithm B for breaking hypothesis 2 with a nonnegligible advantage. B was given $g_p, X_1X_2, Y_1Y_2, g_r, T$, and A simulation $Game_{2,\mathrm{k}-1}$ and $Game_{2,\mathrm{k}}$. □

B random selection $a, a_1, a_2, w \in Z_N$, set $R_0 = g_r^{a_1}$, $R_1 = g_r^{a_2}$, $A_0 = g_p \cdot R_0$, $A_1 = g_p^a \cdot R_1$, and send the public key to A

$$\mathrm{PK} = \left(A_0, A_1, g_r, Y = \widehat{e}(g_p, g_p)^w\right), \tag{A.9}$$

and B knows the master key $MSK = (g_p, a, w)$, next let us explain how B answers the query for the jth key.

For $j < k$, B creates a semi-functional key by uniformly choosing $t_i \in Z_N$, where $i = 1, 2, \ldots, n$, and setting $t = \sum_{i=1}^n t_i$, calculate $D_0 = (Y_1Y_2)^{w-t}, D_i = (Y_1Y_2)^{t_i/a}$. We can notice that this is a distributed semi-functional key.

For $j > k$, B runs the key generation algorithm *KeyGen* to generate the common key.

For $j = k$, B creates a semi-functional key by uniformly choosing $t_i \in Z_N$, where $i = 1, 2, \ldots, n$, and setting $t = \sum_{i=1}^n t_i$, when $y_0 = c(w - t), y_i = ct_i/a$ is calculated as follows:

$$D_0 = T^{w-t},\ D_i = g_p^{t_i/a} g_q^{y_i}. \tag{A.10}$$

This is a semi-functional key. If $T \overset{R}{\longleftarrow} G_p$, it is a normal key.

At some point, A sends two messages of equal length $SymKey_1, SymKey_2$ and two access policies Γ_1, Γ_2 to B. B randomly selects $\beta \in \{0,1\}$ and performs the following actions:

(1) B random choice $s \in Z_N, R_0' \in G_r, s_{i,j} \in Z_N$ and $R_{i,j}' \in G_r$.

(2) B calculated $\tilde{C} = SymKey_\beta \cdot \widehat{e}(g_p^w, X_1X_2), C_0 = X_1X_2 \cdot R_0^s \cdot R_0'$, and when $1 \le i \le n$, $1 \le j \le l$, and $r_{i,j} = s_{i,j}/as$, compute the following:

$$C_{i,j} = \begin{cases} (X_1X_2)^a \cdot R_1^s \cdot R_{i,j}^{'}, v_{i,j} \in W_i; \\ (X_1X_2)^{a \cdot r_{i,j}} \cdot R_1^{s_{i,j}} \cdot R_{i,j}^{'}, \text{otherwise} \end{cases}. \tag{A.11}$$

(3) B sets the challenge ciphertext $CT = (\tilde{C}, C_0, \{C_{i,j}\}_{1 \le i \le n, 1 \le j \le l})$ at this point and sends this to A.

If $T \overset{R}{\longleftarrow} G_p \times G_q$, then let $T = g_p^s g_q^{x_0}$, $\tilde{C} = Symkey_\beta \cdot \widehat{e}(g_p, g_p)^{ws}$, $C_0 = g_p^s g_q^{x_0} \cdot R_0^s \cdot R_0'$, and when $1 \le i \le n, 1 \le j \le l$

$$x_{i,j} = \begin{cases} ax_0,\ v_{i,j} \in W_i \\ ax_0 r_{i,j}, \text{otherwise} \end{cases}, \tag{A.12}$$

calculate

$$C_{i,j} = \begin{cases} g_p^{as} g_q^{x_{i,j}} \cdot R_1^s \cdot R_{i,j}^{'}, v_{i,j} \in W_i \\ g_p^{as_{i,j}} g_q^{x_{i,j}} \cdot R_1^{s_{i,j}} \cdot R_{i,j}^{'}, \text{otherwise} \end{cases}. \tag{A.13}$$

If $T \overset{R}{\longleftarrow} G_p$, B simulation $Game_{2,\mathrm{k}-1}$. If $T \overset{R}{\longleftarrow} G_p \times G_q$, B simulation $Game_{2,\mathrm{k}}$. Finally, B distinguishes the possibility of T by the output of A.

Lemma A.3. *Suppose **G** satisfies Assumption 3, then $Game_{2,\mathrm{p}}$ and $Game_3$ are indistinguishable.*

Proof. Assuming that algorithm A can distinguish between $Game_{2,\mathrm{p}}$ and $Game_3$, we construct an algorithm B that has a nonnegligible advantage for breaking Assumption 3. B is given g_p, $g_p^w X_2, g_p^s Y_2, Z_1Z_2, g_r$, T, and A simulation $Game_{2,\mathrm{p}}$ and $Game_3$. □

B randomly selected $a, a_1, a_2, w \in Z_N$, setting $R_0 = g_r^{a_1}$, $R_1 = g_r^{a_2}, A_0 = g_p \cdot R_0, A_1 = g_p^a \cdot R_1$, and sends the public key to A.

$$PK = \left(A_0, A_1, g_r, Y = \widehat{e}(g_p, g_p^w X_2) = \widehat{e}\left(g_p, g_p\right)^w\right). \tag{A.14}$$

B randomly selected $t_i \in Z_N, i = 1, 2, \ldots, n$, set $t = \sum_{i=1}^n t_i$ to create a semi-functional key, and then calculate $D_0 = (Z_1Z_2)^{w-t}, D_i = (Z_1Z_2)^{t_i/a}$, we can notice that this is a distributed semi-functional key.

At some point, A sends two messages of equal length $SymKey_1, SymKey_2$ and two access policies Γ_1, Γ_2 to B. B randomly selects $\beta \in \{0,1\}$ and performs the following actions:

(1) B random choice $s \in Z_N, R_0' \in G_r, s_{i,j} \in Z_N$ and $R_{i,j}' \in G_r$.

(2) B calculated $\tilde{C} = SymKey_\beta \cdot T, C_0 = g_p^s Y_2 \cdot R_0^s \cdot R_0'$, and when $1 \le i \le n, 1 \le j \le l$ and $r_{i,j} = s_{i,j}/as$, compute the following:

$$C_{i,j} = \begin{cases} \left(g_p^s Y_2\right)^a \cdot R_1^s \cdot R_{i,j}^{'}, v_{i,j} \in W_i; \\ \left(g_p^s Y_2\right)^{a \cdot r_{i,j}} \cdot R_1^{s_{i,j}} \cdot R_{i,j}^{'}, \text{otherwise} \end{cases}. \tag{A.15}$$

(3) B sets the challenge ciphertext $CT = (\tilde{C}, C_0, \{C_{i,j}\}_{1 \le i \le n, 1 \le j \le l})$ at this point and sends this to A. Setting $g_p^s Y_2 = g_p^s g_q^{x_0}, \tilde{C} = SymKey_\beta \cdot T, C_0 = g_p^s g_q^{x_0} \cdot R_0^s \cdot R_0'$ 。when $1 \le i \le n, 1 \le j \le l$ and

$$x_{i,j} = \begin{cases} ax_0, v_{i,j} \in W_i \\ ax_0 r_{i,j}, \text{otherwise} \end{cases}, \tag{A.16}$$

calculate

$$C_{i,j} = \begin{cases} g_p^{as} g_q^{x_{i,j}} \cdot R_1^s \cdot R_{i,j}^{'}, v_{i,j} \in W_i \\ g_p^{as_{i,j}} g_q^{x_{i,j}} \cdot R_1^{s_{i,j}} \cdot R_{i,j}^{'}, \text{otherwise} \end{cases}. \tag{A.17}$$

If $T \overset{R}{\longleftarrow} \widehat{e}(g_p, g_p)^{ws}$, this is a properly distributed semi-functional encryption of $SymKey_\beta$, and B simulates $Game_{2,\mathrm{p}}$; if $T \overset{R}{\longleftarrow} G_T$, this is a properly distributed semi-functional encryption of a random message in G_T, and B simulates $Game_3$. Finally, B distinguishes the possibility of T by the output of A.

Lemma A.4. *Suppose **G** satisfies Assumption 4, then $Game_3$ and $Game_4$ are indistinguishable.*

Proof. Assuming that algorithm A can distinguish between $Game_3$ and $Game_3$, we construct algorithm B that has a nonnegligible advantage for breaking Assumption 4. B is given g_pR_0, $g_p^aR_1$, g_pQ_1, g_p, g_r, T, and A simulation $Game_3$ and $Game_3$. □

B random choice $w \in Z_N$, setting $A_0 = g_p \cdot R_0$, $A_1 = g_p^a \cdot R_1$, and sends the public key to A.

$$PK = \left(A_0, A_1, g_r, Y = \widehat{e}\left(g_p, g_p\right)^w\right). \tag{A.18}$$

B random choice $t_i \in Z_N$, $i = 1, 2, \ldots, n$, setting $t = \sum_{i=1}^n t_i$, create a semi-functional key and then calculate $D_0 = (g_pQ_1)^{w-t}$, $D_i = (g_pQ_1)^{t_i/a}$. If we let $Q_1 = g_q^c$, we can get $D_0 = g_p^{w-t}g_q^{y_0}, D_i = \mathrm{g}_p^{\mathrm{t_i}/a}g_q^{y_i}$, which $y_0 = c(w-t), y_i = ct_i/a$. We can notice that this is a distributed semi-functional key.

At some point, A sends two messages of equal length $SymKey_1, SymKey_2$ and two access policies Γ_1, Γ_2 to B. B randomly selects $\beta \in \{0, 1\}$ and performs the following actions:

(1) B random choice $s \in Z_N, R_0' \in G_r, s_{i,j} \in Z_N$ and $R_{i,j}' \in G_r$.
(2) B calculated $\tilde{C} \xleftarrow{R} G_T, C_0 = g_p^s g_q^{x_0} \cdot R_0^s \cdot R_0'$, and when$1 \leq i \leq n, 1 \leq j \leq l$ compute the following:

$$C_{i,j} = \begin{cases} (T)^s \cdot R_{i,j}' \cdot g_q^{\widetilde{x}_{i,j}}, v_{i,j} \in W_i; \\ (T)^{s_{i,j}} \cdot R_{i,j}' \cdot g_q^{\widetilde{x}_{i,j}}, \text{otherwise} \end{cases}. \tag{A.19}$$

(3) B sets the challenge ciphertext $CT = (\tilde{C}, C_0, \{C_{i,j}\}_{1 \leq i \leq n, 1 \leq j \leq l})$ at this point and sends this to A.

Setting $T = g_p^aQR$ and $Q = g_q^r$, when $1 \leq j \leq l, 1 \leq j \leq l$ and

$$x_{i,j} = \begin{cases} rs + \widetilde{x}_{i,j}, v_{i,j} \in W_i \\ rs_{i,j} + \widetilde{x}_{i,j}, \text{otherwise} \end{cases}, \tag{A.20}$$

calculate

$$C_{i,j} = \begin{cases} g_p^{as} g_q^{x_{i,j}} \cdot R^s \cdot R_{i,j}', v_{i,j} \in W_i; \\ g_p^{as_{i,j}} g_q^{x_{i,j}} \cdot R^{s_{i,j}} \cdot R_{i,j}', \text{otherwise} \end{cases}, \tag{A.21}$$

when $T = g_p^aQR$, B simulates $Game_3$, when $T \xleftarrow{R} G_T$, B simulates $Game_3$, and finally B distinguishes the possibility of T by the output of A.

Data Availability

The [DATA TYPE] data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by the Natural Science Foundation of Hebei Province under grant number F2021201052.

References

[1] D. Zhang, "Analysis and thinking on the application of electronic medical record data," *Digital Technology & Application*, no. 1, pp. 44–46, 2021.
[2] H. Löhr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in *Proceedings of the 1st ACM International Health Informatics Symposium*, pp. 220–229, ACM, 2010.
[3] S. Liu, "Exploration on electronic medical record management system based on cloud computing technology," *Wireless Internet Technology*no. 3, pp. 61-62
[4] T. Feng, F. Kong, C. Liu, R. Ma, and M. Albettar, "Dual verifiable cloud storage scheme based on blockchain," *Journal on Communication*, vol. 42, no. 12, pp. 192–201, 2021.
[5] K. Xu, Y. Fu, W. Chen, and Y. Zheng, "Research progress on blockchain-based cloud storage security mechanism," *Computer Science*, vol. 48, no. 11, pp. 102–115, 2021.
[6] H. Li, Y. Yang, Y. Dai, S. Yu, and Y. Xiang, "Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data," *IEEE Transactions on Cloud Computing*, vol. 8, no. 2, pp. 484–494, 2017.
[7] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2013.
[8] L. Fang, L. Yin, Y. Guo, and B. Fang, "A survey of key technologies in attribute-based access control scheme," *Chinese Journal of Computers*, vol. 40, no. 7, pp. 1680–1698, 2017.
[9] Z. Chen, W. Xu, B. Wang, and H. Yu, "A blockchain-based preserving and sharing system for medical data privacy," *Future Generation Computer Systems*, vol. 124, pp. 338–350, 2021.
[10] T.-F. Lee, H.-Z. Li, and Y.-P. Hsieh, "A blockchain-based medical data preservation scheme for telecare medical information systems," *International Journal of Information Security*, vol. 20, pp. 589–601, 2021.
[11] P. K. Deb, A. Mukherjee, and S. Misra, "CovChain: blockchain-enabled identity preservation and anti-infodemics for COVID-19," *IEEE Network*, vol. 35, no. 3, pp. 42–47, 2021.
[12] S. M. Pournaghi, M. Bayat, and Y. Farjami, "MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption," *Journal of Ambient Intelligence and Humanized*, vol. 11, pp. 4613–4641, 2020.
[13] Z. Zhang, W. Zhang, and Z. Qin, "A partially hidden policy CP-ABE scheme against attribute values guessing attacks with online privacy-protective decryption testing in IoT assisted

cloud computing," *Future Generation Computer Systems*, vol. 123, pp. 181–195, 2021.

[14] R. Du, T. Zhang, and P. Shi, "Ciphertext policy hidden access control scheme based on blockchain and supporting data sharing," *Journal on Communications*, vol. 6, pp. 168–178, 2022.

[15] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in *Applied Cryptography and Network Security*, vol. 5037 of *Lecture Notes in Computer Science*, pp. 111–129, Springer, Berlin Heidelberg, 2008.

[16] Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: efficient policy-hiding attribute-based access control," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2130–2145, 2018.

[17] S. Gao, G. Piao, J. Zhu, X. Ma, and J. Ma, "Trustaccess: a trustworthy secure ciphertext-policy and attribute hiding access control scheme based on blockchain," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5784–5798, 2020.

[18] D. Ivan, "Moving toward a blockchain-based method for the secure storage of patient records," in *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*, pp. 1–11, ONC/NIST, Gaithersburg, Maryland, United States, 2016.

[19] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-based medical records secure storage and medical service framework," *Journal of Medical Systems*, vol. 43, no. 1, pp. 1–9, 2019.

[20] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data," in *Proceedings of IEEE Open & Big Data Conference*, vol. 13, pp. 1–13, IEEE, 2016.

[21] Q. Xia, E. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: blockchain-based data sharing for electronic medical records in cloud environments," *Information-an International Interdisciplinary Journal*, vol. 8, no. 2, Article ID 44, 2017.

[22] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable Cities and Society*, vol. 39, pp. 283–297, 2018.

[23] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," *AMIA Annual Symposium Proceedings*, vol. 2017, pp. 650–659, 2017.

[24] L. Zhang, J. Liu, Y. Tao et al., "Blockchain-based encrypted access control scheme for medical information attributes," *Journal of Cyber Security*, vol. 8, no. 1, 2023.

[25] X. Sun, F. Xin, D. Wang, and B. Cheng, "A study of case sharing blockchain model for research organizations," *Journal of the Hebei Academy of Sciences*, no. 2, pp. 24–28, 2023.

[26] G. Han, J. Wang, W. Luo, and Y. Lu, "Research on access control and secure sharing of medical data during public health events," *Journal of Cyber Security*, vol. 8, no. 1, pp. 40–54, 2023.

[27] K. Riad, R. Hamza, and H. Yan, "Sensitive and energetic IoT access control for managing cloud electronic health records," *IEEE Access*, vol. 7, pp. 86384–86393, 2019.

[28] J. Wei, X. Chen, X. Huang, X. Hu, and W. Susilo, "RS-HABE: revocable-storage and hierarchical attribute-based access scheme for secure sharing of e-health records in public cloud," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, pp. 2301–2315, 2019.

[29] S. Liu, J. Yu, Y. Xiao, Z. Wan, S. Wang, and B. Yan, "BC-SABE: blockchain-aided searchable attribute-based encryption for cloud-IoT," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 7851–7867, 2020.

[30] R. Guo, G. Yang, H. Shi, Y. Zhang, and D. Zheng, "O^3 -R-CP-ABE: an efficient and revocable attribute-based encryption scheme in the cloud-assisted IoMT system," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8949–8963, 2021.

[31] J. Li, S. Qin, F. Gao, and D. Sun, "Controllable and regulated privacy protection scheme for controlled and regulated transactions of blockchain organizations based on attribute encryption," *Netinfo Security*, vol. 23, no. 12, pp. 103–112, 2023.

[32] T. Feng, Q. Chen, J. Fang, and J. Shi, "A blockchain data sharing scheme based on localized differential privacy and attribute-based searchable encryption," *Journal on Communications*, vol. 44, no. 5, pp. 224–233, 2023.

[33] J. Lai, R. H. Deng, and Y. Li, "Fully secure cipertext-policy hiding CP-ABE," in *Information Security Practice and Experience*, vol. 6672 of *Lecture Notes in Computer Science*, pp. 24–39, Springer, Berlin Heidelberg, 2011.

[34] J. Hur, "Attribute-based secure data sharing with hidden policies in smart gird," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 11, pp. 2171–2180, 2013.

[35] Y. Michalevsky and M. Joye, "Decentralized policy-hiding ABE with receiver privacy," in *Computer Security. ESORICS 2018*, vol. 11099 of *Lecture Notes in Computer Science*, pp. 548–567, Springer International Publishing, Cham, 2018.

[36] C. Dai, H. Luan, X. Yang, X. Guo, Z. Lu, and B. Niu, "Overview of blockchain technology," *Computer Science*, no. S2, pp. 500–508, 2021.

[37] Q. Yao and D.-W. Zhang, "Survey on identity management in blockchain," *Journal of Software*, vol. 32, no. 7, pp. 2260–2286, 2021.

[38] Z. Zhang, G. Wang, J. Xu, and X. Du, "Survey on data management in blockchain systems," *Journal of Software*, vol. 31, no. 9, pp. 2903–2925, 2020.

[39] S. Jin, X. Zhang, J. Ge et al., "Overview of blockchain consensus algorithm," *Journal of Cyber Security*, no. 2, pp. 85–100, 2021.

[40] M. Zheng, H. Wang, H. Liu, and C. Tan, "Survey on consensus algorithms of blockchain," *Netinfo Security*, vol. 7, pp. 8–24, 2019.

[41] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in *Theory of Cryptography*, vol. 3378 of *Lecture Notes in Computer Science*, pp. 325–341, Springer, Berlin, Heidelberg, 2005.

[42] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in *Advances in Cryptology–EUROCRYPT 2008*, vol. 4965 of *Lecture Notes in Computer Science*, pp. 146–162, Springer, Berlin Heidelberg, 2008.

[43] G. Xu, H. Li, S. Liu, M. Wen, and R. Lu, "Efficient and privacy-preserving truth discovery in mobile crowd sensing systems," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 3854–3865, 2019.

[44] J. Lai, R. H. Deng, and Y. Li, "Expressive CP-ABE with partially hidden access structures," in *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, pp. 18-19, ACM, 2012.

[45] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: attribute-based encryption and (Hierarchical) inner product encryption," in *Advances in Cryptology-EUROCRYPT 2010*, vol. 6110 of *Lecture Notes in Computer Science*, pp. 62–91, Springer, Berlin Heidelberg, 2010.

[46] A. Lewko and B. Waters, "New proof methods for attribute-based encryption: achieving full security through selective techniques," in *Advances in Cryptology–CRYPTO 2012*, vol. 7417 of *Lecture Notes in Computer Science*, pp. 180–198, Springer, Berlin Heidelberg, 2012.

[47] T. V. X. Phuong, G. Yang, and W. Susilo, "Hidden ciphertext policy attribute-based encryption under standard assumptions," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 1, pp. 35–45, 2016.

[48] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *Proceedings of the 16th ACM conference on Computer and Communications Security*, pp. 121–130, ACM, 2009.

[49] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Advances in Cryptology–EUROCRYPT 2011*, vol. 6632, pp. 568–588, Springer, Berlin, Heidelberg, 2011.

[50] B. Waters, "Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions," in *Advances in Cryptology-CRYPTO 2009*, vol. 5677 of *Lecture Notes in Computer Science*, pp. 619–636, Springer, Berlin, Heidelberg, 2009.