IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 9, 2020, accepted February 19, 2020, date of publication February 27, 2020, date of current version March 16, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2976894

Medical Data Sharing Scheme Based on Attribute Cryptosystem and Blockchain Technology

XIAODONG YANG[1], (Member, IEEE), TING LI[1], XIZHEN PEI[1], LONG WEN[1], AND CAIFEN WANG[1,2]

[1]College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China
[2]College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China

Corresponding author: Caifen Wang (wangcfen@126.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61662069 and Grant 61562077, in part by the China Postdoctoral Science Foundation under Grant 2017M610817, in part by the Science and Technology Project of Lanzhou City under Grant 2013-4-22, and in part by the Foundation of Northwest Normal University under Grant NWNU-LKQN-14-7.

ABSTRACT Electronic medical data have significant advantages over paper-based patient records when it comes to storage and retrieval. However, most existing medical data sharing schemes have security risks, such as being prone to data tampering and forgery, and do not support the ability to verify the authenticity of the data source. To solve these problems, we propose a medical data sharing scheme based on attribute cryptosystem and blockchain technology in this paper. First, the encrypted medical data are stored in the cloud, and the storage address and medical-related information are written into the blockchain, which can ensure efficient storage and eliminate the possibility of irreversible modification of the data. Second, the proposed scheme combines attribute-based encryption (ABE) and attribute-based signature (ABS), which achieves the sharing of medical data in many-to-many communications. The ABE achieves data privacy and fine-grained access control, and the ABS verifies the authenticity of the source of the medical data while protecting the signer's identity. Moreover, the data user outsources most of the operations of medical data ciphertext decryption to the cloud service provider (CSP), which can greatly reduce the computational burden. Finally, results of the analysis show that our scheme satisfies the requirements for confidentiality and unforgeability in the random oracle model, and that the proposed scheme offers higher computational performance than other similar schemes.

INDEX TERMS Attribute-based cryptosystem, blockchain, confidentiality, electronic medical data, unforgeability.

I. INTRODUCTION

Traditional paper-based medical records [1] contain patient information, such as personal medical history, prescriptions, immunizations, results of examination, medical images, and family history of genetic diseases. However, it was difficult and time-consuming for two or more medical institutions to share paper-based medical data. A solution to this problem is to share the patient's medical data electronically. Medical data in digital format enable the long-term preservation and on-demand recall of medical data, and they can help doctors make more accurate diagnoses of patients' conditions. Nevertheless, the skyrocketing amount of medical data requires costly storage overhead. When electronic medical data are distributed between different medical institutions across an open network, it is easy for attacks such as tampering, monitoring, and forgery to take place.

Cloud storage technology can store massive amounts of electronic medical data with powerful computation capabilities and low cost. More and more users and medical institutions are uploading medical data to the cloud for storage and sharing. This can reduce the cost of local storage of medical data and enable users to access shared medical data anytime and anywhere. Several cloud-based strategies for medical data sharing have been proposed [2]–[4]. To guarantee the security of data, Cheng *et al.* [2] designed a method to cut big data into a number of ordered data columns and then place these data on a variety of cloud servers. Shen *et al.* [3] proposed a data storage scheme to verify data integrity and security, which can detect whether data have been tampered with before they are downloaded. Xhafa *et al.* [4] presented a medical record system based on the cloud, which used

The associate editor coordinating the review of this manuscript and approving it for publication was Shuiguang Deng.

attribute-based encryption (ABE) to encrypt medical data based on patients' conditions, without exposing the detailed description of the symptoms and the department of the doctor. These schemes [2]–[4] are highly dependent on the cloud service provider (CSP). On the one hand, the CSP may delete data that users have rarely or never accessed to save space for storing other users' data, thereby earning more revenue. On the other hand, the data stored in the cloud may be damaged due to the failure of the cloud server, management errors or malicious attacks; however, the CSP may intentionally hide the fact of data loss to maintain its reputation. Therefore, we can conclude that the cloud makes it convenient for medical institutions to share electronic medical data, but the data stored in the cloud are subject to tampering, forgery, and being accessed by unauthorized individuals.

Blockchain is an emerging Internet database technology characterized by decentralization, transparency, and data non-tamperability, which was first proposed by [5]. For blockchain technology, there is no need to use third parties to store data for us reliably, nor to worry about the unavailability of data. Consequently, it can avoid the security problem of data in the cloud. Many researchers have recently conducted studies on the application of blockchain in the medical field. To achieve the secure sharing of medical data, Peterson *et al.* [6] proposed a consensus mechanism based on blockchain technology, but the communication overhead of node consensus is high. Liang *et al.* [7] presented a secure data transmission scheme based on the Fabric blockchain to improve the security of data transmission and reduce the communication overhead. Ekblaw [8] presented a management system for electronic medical records that ensures the accuracy of medical records by using the non-tamperability of blockchain. However, scheme [8] does not specify an access control policy for data access, which may lead to the accidental exposure of medical records. Scheme [9] achieves the management of distributed medical data by utilizing smart contracts and access control, but the use of the proof-of-work consensus mechanism results in a high computational cost for blockchain. Siyal *et al.* [10] analyzed the challenges faced by the application of blockchain in the field of medicine, and argued that the public verifiability of blockchain allows electronic medical records to be verified without any third party. Nevertheless, scheme [10] cannot ensure the reliability of the data source, resulting in the decrease of data availability. Sun *et al.* [11] applied an attribute-based signature (ABS) scheme to a blockchain system, which enables medical data to be shared between medical institutions and the authenticity of the data source to be verified. In this mechanism, the signer's attributes are verified and the identity of the signer is protected simultaneously. However, with the increase of medical data, the blockchain system brings about a large storage overhead as well as computational overhead. To store medical data efficiently and securely, Wang and Song [12] presented a secure medical data storage system that combines cloud storage and blockchain technology, thereby significantly improving the supervision of the system and ensuring the integrity and traceability of medical data. However, the computational overhead was not decreased significantly. In this paper, we propose the first open medical data sharing scheme based on blockchain and cloud storage technology, which can allow multiple users to share and access medical data at the same time, and satisfy the requirements for confidentiality, integrity, non-tamperability, anonymity, and verifiability simultaneously.

A. OUR CONTRIBUTIONS

In this paper, we design a medical data sharing scheme based on blockchain technology and attribute-based cryptosystem, which provides efficient storage and secure sharing services for medical data. Our contributions are as follows.

- We design a new medical data sharing scheme, which submits the encrypted medical data to the cloud and writes corresponding storage address and medical-related information into the blockchain. This can ensure efficient storage of medical data and prevent the CSP from tampering with the data.
- The proposed scheme achieves the confidentiality and privacy of medical data. In our scheme, the patient formulates specific access policies and authorizes doctors to encrypt medical data by using ABE, which can ensure flexible access control to cloud medical data and enable the patient to fully participate in the sharing of medical data.
- Our scheme can guarantee the integrity of the medical data and verify the authenticity of the medical data source without revealing the patient's identity or compromising its privacy. The ABS protocol permits the signer to sign medical data by using a set of attributes rather than his or her identity, which plays a very important role in data authentication and identity-privacy preservation.
- The proposed scheme has lower computation overhead than similar schemes. Based on the outsourced decryption mechanism, the data user entrusts the CSP to perform the partial decryption of the medical data ciphertext. Therefore, the data user only needs to execute simple calculations to complete the decryption operation, thereby reducing the computational burden on users who access data. In addition, our scheme provides a verification function for transformed ciphertext, which can prevent malicious attacks in the cloud and ensure the correctness of the transformed ciphertext.
- Our scheme can resist the chosen ciphertext attack (CCA) under the modified decisional Diffie-Hellman (MDDH) assumption. Meanwhile, the proposed scheme satisfies the requirements of unforgeability and anonymity.

B. ORGANIZATION

The remainder of this paper is organized as follows. Section II introduces related work. Section III reviews some

preliminaries, including bilinear maps, linear secret-sharing schemes (LSSS), AND gate policy, and MDDH assumption. The system model and detailed description of our scheme are presented in Sections IV and V, respectively. Section VI analyzes the security and performance of our scheme from the perspectives of confidentiality, unforgeability, and anonymity. Section VII presents our conclusion.

II. RELATED WORK

This section is mainly concerned with the cryptographic technology used to achieve secure sharing of medical data. Doukas *et al.* [13] used the traditional public key infrastructure (PKI) technology to encrypt medical data, avoiding attacks by eavesdroppers, but this scheme faced huge certificate management overhead. Scheme [14] achieved simple role-based access control by using identity-based encryption (IBE), but there is a problem of the key escrow arrangement. Schemes [13], [14] both realize many-to-one encryption; that is, only one user can decrypt data. To address these issues, Li *et al.* [15] proposed a medical data sharing scheme based on attribute encryption, in which medical data are encrypted according to the users' set of attributes, so that multiple users with corresponding keys can decrypt the data. Moreover, this makes data encryption and key management more efficient. With the development of ABE, the research related to ABS began to appear. Scheme [16] designed a medical data sharing scheme based on attribute signature, which can verify the source and integrity of medical data and protect the privacy of the signer. To reduce the computational burden on data users, scheme [17] applies an outsourcing calculation mechanism to share medical data.

Shamir [18] first introduced the notion of IBE. Boneh and Franklin [19] put forward the first secure IBE scheme by employing bilinear mapping. On the basis of [18], [19], Sahai and Waters [20] constructed a fuzzy IBE scheme, and at the same time extended their ideas to propose a notion of ABE. In order to express a more flexible access strategy, Goyal *et al.* [21] presented an attribute-based key policy encryption scheme, but the scheme only supports monotonic access control structures. Ostrovsky *et al.* [22] proposed a logic inconsistent ABE scheme and extended the access control structure based on attribute schemes from monotonic to non-monotonic. However, data owners lack control over access strategies. Cheung and Newport [23] presented an attribute-based ciphertext policy encryption scheme, which takes the user's identity information as the attribute, and allows the data owner formulate the access control policy to fully control the access policy. The access structure of this scheme supports the logical relationship between positive and negative attributes, which proved to be resistant to ciphertext forgery attack. Nevertheless, in this scheme, the access structure is simple and the public parameters are long, so its efficiency is low. Subsequently, many ABE schemes with special properties appeared [24]–[27], and the schemes [26], [27] were extended and applied in practice.

Yang *et al.* [28] first introduced a fuzzy identity-based signature scheme and proved the unforgeability of the scheme by using the computational Diffie-Hellman assumption. Maji *et al.* [29] put forward an ABS scheme that can protect the signer's identity and resist collusion attacks by different users. However, the computing performance of this scheme is relatively low. In addition, this scheme only resists selective message attacks under the general group model. To enhance the security of this scheme, Li *et al.* [30] presented two ABS schemes that support the threshold structure. Lewko and Waters [31] presented a distributed attribute-based encryption (DABE) scheme, which can be applied to distributed networks. Inspired by [31], Sun *et al.* [11] presented a decentralizing attribute-based signature (DABS) scheme, which is applicable to the blockchain system.

Green *et al.* [32] introduced an attribute-based encryption with outsourced decryption (OD-ABE) scheme, which delegates a large amount of decryption calculation to the proxy server, and the proxy server sends the partially decrypted ciphertext to the subscriber who can decrypt the ciphertext with only a small amount of computation. However, the proxy server is considered to be semi-honest. In order to ensure that the proxy server correctly performs the partial decryption process, Lai *et al.* [33] proposed a verifiable OD-ABE scheme. Li *et al.* [34] presented a checkable OD-ABE scheme that can ensure the validity of the message and outsourced calculation results. At the same time, many OD-ABE schemes [35]–[37] were proposed, but these schemes cannot achieve CCA security. Zuo *et al.* [38] proposed a CCA secure OD-ABE scheme and proved its security. However, designing a secure and efficient ABE scheme remains an open challenge.

III. PRELIMINARIES

In this section, we review the notations and definitions related to the proposed scheme.

A. BILINEAR MAPS

Let G and G_T be two multiplicative cyclic groups of prime order p, where g is a generator of G. The map $\hat{e} : G \times G \rightarrow G_T$ is said to be a bilinear map if it satisfies the following properties [39].

(1) Bilinear: There is $\hat{e}(g^a, g^b) = \hat{e}(g, g)^{ab}$ for any $a, b \in Z_p$.

(2) Non-degenerate: $\hat{e}(g, g) \neq 1$.

(3) Computable: For any $g_1, g_2 \in G$, there is an efficient algorithm for calculating $\hat{e}(g_1, g_2)$.

B. LINEAR SECRET SHARING SCHEME

The aim of the linear secret-sharing scheme (LSSS) [40] is to split the secrets in an appropriate way. Then, each share is managed by different participants. A single participant cannot recover the secret information, and only a few participants can cooperate to recover the secret. The specific description is as follows.

(1) **Secret generation**: The secret distributor chooses a matrix M with x rows and j columns named the

share-generation. Suppose that vector $v = (s, r_2, \ldots, r_j)$ is the transpose of matrix, where $s \in Z_p$ is the secret value to be shared and $r_2, \ldots, r_j \in Z_p$ are random elements.

(2) **Secret distribution**: The secret distributor assigns the shared secret value s to x members $U_1, \ldots, U_x$, where the secret share owned by the k-th member U_k is $M_k \times v$, and the k-th row of the matrix M is identified as the function $\rho(k)$.

(3) **Secret recovery**: Let K be the authorization set, and $\{\lambda_i\}_{k \in K}$ represents the secret shares, where $K \subseteq \{1, \ldots, x\}$ is defined as $K = \{k|\rho(k) \in S\}$. There exists a constant $\{\omega_k \in Z_p\}_{x \in K}$, and k authorized users can recover the secret value s by using $\{\lambda_i\}$.

C. AND-GATE POLICY

$N = \{1, \ldots, n\}$ represents a set of attributes, where the attribute $i \in N$. The attribute $+i$ and $-i$ denote a positive attribute and a negative attribute, respectively. $\Lambda = \wedge_{i \in I} \underset{\sim}{i}$ means an access structure, where $I \subseteq N$, $\underset{\sim}{i} = +i$ or $\underset{\sim}{i} = -i$ [23].

D. MODIFIED DECISIONAL DIFFIE-HELLMAN (MDDH) ASSUMPTION

The MDDH assumption is to distinguish between $(g, g^a, \hat{e}(g, g)^b, \hat{e}(g, g)^{ab})$ and $(g, g^a, \hat{e}(g, g)^b, \hat{e}(g, g)^c)$, where $a, b, c \in Z_p$.

Definition 1: We say that the MDDH assumption holds if there is no polynomial time algorithm that solves the MDDH problem with a non-negligible probability [41].

IV. MODEL OF SYSTEM

There are six entities in the system model of our scheme, such as attribute authority organization (AAO), patients, hospitals, blockchain system, CSP, and medical data users (such as medical institutions and insurance companies), as illustrated in Figure 1.

(1) The AAO is mainly responsible for distributing the corresponding attribute signature key $SIK_{i,GID}$, transformed key tk and private key d to the patient, medical data users and hospitals respectively.

(2) The patient formulates the access control policy Λ and sends Λ to the hospitals. Then, the patient generates the signature σ of medical-related information m_0 according to the LSSS. Finally, the patient sends σ and m_0 to the data pool.

(3) The hospital encrypts the medical data according to the access structure Λ specified by the patient and sends the ciphertext CT to the data pool.

(4) The blockchain system consists of a data pool, blockchain and consensus network. The data pool stores medical data ciphertext, medical-related information and its signature. To improve the security of the medical data, the consortium blockchain is constructed in the system. The alliance members include medical data users, hospitals, research institutes and accounting nodes, and they maintain the blockchain jointly. The consortium blockchain is responsible for storing medical-related information and the address of encrypted medical data and ensuring that the content on the blocks is immutable. In the consensus network, the proof-of-stake (PoS) mechanism is used in the consensus process to ensure the security of the blockchain ledger. The consensus nodes first implement the PoS mechanism to select the accounting nodes, which can realize the distributed consensus of the blockchain. Next, the accounting nodes send the medical data ciphertext to the cloud and obtain the data access address from the cloud. Finally, the accounting nodes write the storage address of cloud medical data ciphertext and medical-related information to the blockchain. Compared with the distributed server, blockchain has the characteristics of decentralization, verifiability and immutability, which are essential in our system.

(5) The CSP mainly stores medical data ciphertext and sends the address of the ciphertext to the bockchain. And the CSP is also authorized by the data users to complete a partial decryption of the encrypted medical data.

(6) Medical data users initiate the medical data access requests by submitting their attributes set to the blockchain system. If the verification is passed, data users obtain the medical data ciphertext address sent by the accounting node. Then, the data users send the address and the transformed key to the CSP, which is authorized to partially decrypt the medical data ciphertext. Finally, the users completely decrypt the medical data ciphertext by using the retrieval key.

V. A NEW MEDICAL DATA SHARING SCHEME

A. DESCRIPTION OF THE PROGRAM

Based on OD-ABE [38] and DABS [11], a medical data sharing scheme based on blockchain technology and attribute cryptosystem is proposed in this section.

- **System Setup:** The AAO chooses two multiplicative cyclic groups G and G_T of prime p, a generator g of G and a bilinear map $\hat{e} : G \times G \rightarrow G_T$. Next, it chooses five hash functions $H_1 : \{0,1\}^{2l} \rightarrow Z_p$, $H_2 : G_T \rightarrow \{0,1\}^l$, $H_3 : \{0,1\}^l \rightarrow \{0,1\}^l$, $H_4 : \{0,1\}^* \rightarrow G$ and $H_5 : \{0,1\}^* \rightarrow G_T$, where l is the length of the medical data. Then, it defines a set of attributes $N = \{1, \ldots, n\}$ and selects $\varphi, t_1, \ldots, t_{3n} \in Z_p$ randomly to calculate $\phi = \hat{e}(g, g)^{\varphi}$ and $T_i = g^{t_i}$, where $i \in \{1, \ldots, 3n\}$. Finally, it keeps the master key $msk = (\varphi, t_1, \ldots, t_{3n})$ secretly, and sets $PP = (\hat{e}, p, g, G, G_T, \phi, T_1, \ldots, T_{3n}, H_1, H_2, H_3, H_4, H_5)$ as the public parameters.
- **Key Generation:** When users register in the system, they can get the corresponding key from the AAO. *Phase 1 (Generation of Private Key):* After receiving the attribute set $S_f = \{S_{f1}, \cdots, S_{fw}\} \subseteq N$ sent by a hospital, the AAO generates the corresponding attribute private key. The detailed steps are as follows.
  1) Randomly choose $r_i \in Z_p$, where $i \in [1, n]$, and calculate $r = \sum_{i=1}^{n} r_i \bmod p$ and $\hat{D} = g^{\varphi - r}$.
  2) Calculate $D_i = \begin{cases} g^{r_i/t_i}, & i \in S_f \\ g^{r_i/t_{n+i}}, & i \notin S_f \end{cases}$ and $F_i = g^{r_i/t_{2n+i}}$, where $i \in [1, n]$.

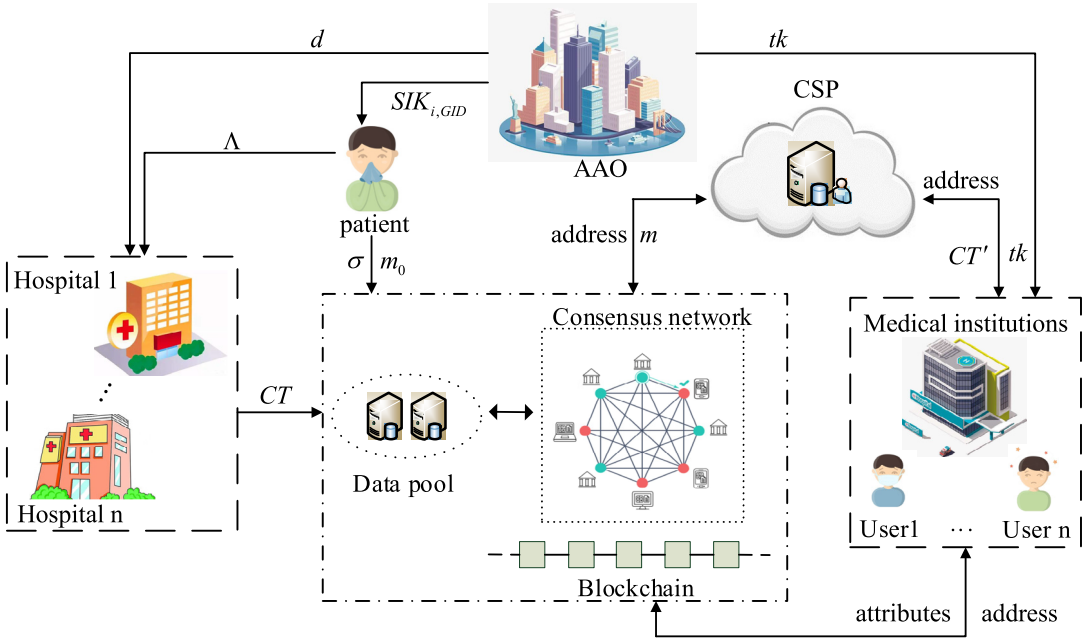

FIGURE 1. System model.

3) Generate a private key $d = \{\hat{D}, (D_i, F_i)\}$ associated with the attribute $S_\int$, where $i \in [1, n]$, and send d to the hospital.

Phase 2 (Generation of Signature Key): After receiving the attribute set $S_U = \{S_{U1}, \cdots, S_{Uw}\} \subseteq N$ and the globally verified identifier GID sent by a patient, the AAO generates a corresponding signature key. This phase includes the following two steps.

1) Randomly select $\alpha_i, \gamma_i \in Z_p$ for each attribute i to calculate $VK = \{\hat{e}(g, g)^{\alpha_i}, g^{\gamma_i}\}$ and $SIK = \{\alpha_i, \gamma_i\}$ where $i \in [1, n]$.
2) Calculate the signature key $SIK_{i,GID} = \{g^{\alpha_i}, H_4(GID)^{\gamma_i}$ corresponding to each GID and send $SIK_{i,GID}$ to the patient, where $i \in [1, n]$.

Phase 3 (Generation of the Outsourced Decryption Key): The phase of generating outsourced decryption key by medical data users and the AAO is as follows:

1) The medical data users first select a random element $\eta \in Z_p$ as the retrieval key rk. Then, they send the private key $d = \{\hat{D}, (D_i, F_i)\}$ with the attribute set $S_\int$ to the AAO and obtain the transformed key $tk = (\hat{D}^\eta, \{(D_i^\eta, F_i^\eta) | i \in [1, n]\})$ generated by the AAO.
2) The medical data users secretly save the outsourced decryption key $ok = \{tk, rk\}$.

- **Medical Data Upload**

Phase 1 (Signature Generation): First, the patient chooses an AND gate $\Lambda = \wedge_{i \in I} \underset{\sim}{i}$ of medical data m, where $I \subseteq N$, the attribute $i \in I$ and it satisfies $\underset{\sim}{i} = +i$ or $\underset{\sim}{i} = -i$. Then, medical-related information m_0 (including medical record type, diagnostic date, and access control structure) is generated. Finally, the patient generates the signature σ of m_0 by the following steps.

1) First, select an $x \times j$ access matrix M with function ρ maps each row of matrix M to an attribute and randomly select $z \in Z_p$ and a vector $\nu \in Z_p^x$, where z is the first element of the vector ν. Then, define M_k as the k line of matrix M and calculate $\mu_k = M_k \cdot \nu$. Finally, randomly select a vector $\omega \in Z_p^x$, where the first element of ω is 0, and calculate $\omega_k = M_k \cdot \omega$.
2) For each M_k, select a random element $\tau_k \in Z_p$.
3) Calculate $\sigma_0 = \hat{e}(g, g)^{\eta \cdot H_5(m_0)}$, $\sigma_1 = H_4(GID)^{\tau_k}$ and $\sigma_2 = \frac{\hat{e}(g,g)^{\mu_k} \cdot \hat{e}(H_4(GID), g^{\omega_k})}{\hat{e}(g^{\alpha_{\rho(M_k)}}, g) \cdot \hat{e}(H_4(GID)^{\gamma_{\rho(M_k)}}, g^{\tau_k})}$.
4) Generate the signature $\sigma = (\sigma_0, \sigma_1, \sigma_2)$ of m_0 and send σ to the data pool.

Phase 2 (Ciphertext Generation): After receiving the access structure $\Lambda = \wedge_{i \in I} \underset{\sim}{i}$ sent by the patient, the hospital generates the ciphertext of the medical data m by the following steps.

1) Randomly choose $\zeta \in \{0, 1\}^l$ and calculate $\partial = H_1(\zeta || m)$, $\bar{C}_1 = \zeta \oplus H_2(\phi^\partial)$, $\bar{C}_2 = m \oplus H_3(\zeta)$, $\bar{C}_3 = g^\partial$, and

$$C_i = \begin{cases} T_i^{\partial}, & i \in I \wedge \underset{\sim}{i} = +i \\ T_{n+i}^{\partial}, & i \in I \wedge \underset{\sim}{i} = -i \\ T_{2n+i}^{\partial}, & i \in N \backslash I. \end{cases}$$

2) Calculate $\bar{C}_4 = H_4(\Lambda || \bar{C}_1 || \bar{C}_2 || \bar{C}_3 || C_1 || \ldots || C_n)^\partial$.
3) Send ciphertext $CT = (\Lambda, \bar{C}_1, \bar{C}_2, \bar{C}_3, \bar{C}_4, \{C_i\}_{i \in N})$ of the medical data m to the data pool.

Phase 3 (Data Upload): After receiving the ciphertext CT of the medical data m and the signature σ of the medical-related information m_0, the accounting nodes perform the following three steps.

1) Calculate τ_k by $\sum_k \tau_k M_k = (1, 0, \ldots, 0)$, then verify that $\sigma_0^{\frac{1}{H_3(m_0)}} = \prod_k (\hat{e}(g, g)^{\alpha_{\rho(M_k)}} \cdot \hat{e}(\sigma_1, g^{\gamma_{\rho(M_k)}}) \cdot \sigma_2)^{\tau_k}$ holds or not. If the equation holds, perform the following steps; otherwise, discard this data.
2) Upload the ciphertext CT to the cloud.
3) Write medical-related information m_0 and the address of ciphertext CT to the blockchain.

- **Medical data access**

Phase 1 (Outsourced Decryption of Medical Data): After receiving the transformation key tk and the ciphertext CT of medical data submitted by the medical data users, the CSP performs the following three steps.

1) Check whether the following equations hold: $\hat{e}(\bar{C}_3, H_4(\Lambda||\bar{C}_1||\bar{C}_2||\bar{C}_3||C_1||\cdots||C_n)) = \hat{e}(g, \bar{C}_4)$, $\hat{e}(\bar{C}_3, T_i) = \hat{e}(g, C_i)$ for $i \in I \wedge \dot{i} = +i$, $\hat{e}(\bar{C}_3, T_{n+i}) = \hat{e}(g, C_i)$ for $i \in I \wedge \dot{i} = -i$, and $\hat{e}(\bar{C}_3, T_{2n+i}) = \hat{e}(g, C_i)$ for $i \in N \backslash I$. If one of the above equations does not hold, the operation is aborted; otherwise, perform steps 2 and 3.
2) Calculate $\bar{C}_5 = \prod_{i \in N \backslash I} \hat{e}(C_i, F_i^{\eta}) \cdot \prod_{i \in I} \hat{e}(C_i, D_i^{\eta}) \cdot \hat{e}(\bar{C}_3, \hat{D}^{\eta}) = \hat{e}(g, g)^{\varphi \cdot \partial \cdot \eta}$.
3) Generate the transformed ciphertext $CT' = (\bar{C}_1, \bar{C}_2, \bar{C}_5)$, and send CT' to the data users.

Phase 2 (Decryption of Medical Data): After receiving transformed ciphertext CT', data users perform the following steps.

1) Check $\bar{C}_1 = \zeta \oplus H_2(\phi^{H_1(\zeta||m)})$ and $\phi^{H_1(\zeta||m)} = \bar{C}_5^{1/\eta}$ hold or not. If one of the above equations does not hold, the operation is aborted; otherwise, step 2 is performed.
2) Obtain m by calculating $\zeta = \bar{C}_1 \oplus H_2(\bar{C}_5^{1/\eta})$ and $m = \bar{C}_2 \oplus H_3(\zeta)$.

B. CORRECTNESS

Suppose that a patient's global identity is GID, its attributes make up the matrix M, and its signature of medical-related information is $\sigma = (\sigma_0, \sigma_1, \sigma_2)$. The correctness of the patient's signature can be verified by the following equation:

$$\begin{aligned}
&\prod_k (\hat{e}(g, g)^{\alpha_{\rho(M_k)}} \cdot \hat{e}(\sigma_1, g^{\gamma_{\rho(M_k)}}) \cdot \sigma_2)^{\tau_k} \\
&= \prod_k (\hat{e}(g, g)^{\alpha_{\rho(M_k)}} \cdot \hat{e}(H_4(GID)^{\tau_k}, g^{\gamma_{\rho(M_k)}}) \\
&\quad \cdot \frac{\hat{e}(g, g)^{\mu_k} \cdot \hat{e}(H_4(GID), g^{\omega_k})}{\hat{e}(g^{\alpha_{\rho(M_k)}}, g) \cdot \hat{e}(H_4(GID)^{\gamma_{\rho(M_k)}}, g^{\tau_k})})^{\tau_k} \\
&= \prod_k (\hat{e}(g, g)^{\mu_k} \cdot \hat{e}(H_4(GID), g)^{\omega_k})^{\tau_k}.
\end{aligned}$$

Since $\mu_k = M_k \cdot \nu$, $\omega_k = M_k \cdot \omega$, $\nu \cdot (1, 0, \ldots, 0) = z$ and $\omega \cdot (1, 0, \ldots, 0) = 0$, we have

$$\prod_k (\hat{e}(g, g)^{\mu_k} \cdot \hat{e}(H_4(GID), g)^{\omega_k})^{\tau_k} = \hat{e}(g, g)^z = \sigma_0^{\frac{1}{H_5(m_0)}}.$$

VI. SECURITY AND PERFORMANCE ANALYSIS

A. SECURITY ANALYSIS

1) CONFIDENTIALITY

Theorem 1: The proposed scheme satisfies confidentiality in the random oracle model if the MDDH assumption holds.

Proof: We use the proof method of Zuo *et al.* [38] to prove the security of our scheme. If there exists an adversary $\mathcal{A}$ that breaks the confidentiality of the proposed scheme with a non-negligible probability ε, then there is an algorithm $\mathcal{B}$ that can solve the MDDH problem. An MDDH instance $(g, \mathbf{A} = g^a, \mathbf{B} = \hat{e}(g, g)^b, \mathbf{Z}) \in G^2 \times G_T^2$ is given, $\mathcal{B}$ performs a security game with $\mathcal{A}$ to determine whether $\mathbf{Z} = \hat{e}(g, g)^{ab}$. The following proves that the confidentiality in our scheme can be reduced to the hardness of the MDDH problem under the chosen ciphertext attack.

Initialization: After receiving the challenge access structure $\Lambda^* = \wedge_{i \in I} \dot{i}$ sent by the adversary $\mathcal{A}$, $\mathcal{B}$ randomly selects $\varphi, t_1, \ldots, t_{3n} \in Z_p$, and calculates $\phi = \hat{e}(g, g)^{\varphi}$ and $T_i = g^{t_i}$, where $i \in [1, 3n]$.

Phase 1: $\mathcal{A}$ initiates the following hash queries, and $\mathcal{B}$ responds as follows.

- H_1-queries: $\mathcal{B}$ creates list L_1 (initially empty). $\mathcal{A}$ sends $V_1 \in \{0, 1\}^{2l}$ to $\mathcal{B}$. If (V_1, h_1) exists in list L_1, $\mathcal{B}$ returns h_1 to $\mathcal{A}$. Otherwise, $\mathcal{B}$ randomly selects $h_1 \in Z_p$ to send $\mathcal{A}$ and adds (V_1, h_1) to list L_1.
- H_2-queries: $\mathcal{B}$ creates a list L_2 (initially empty). $\mathcal{A}$ sends $V_2 \in G_T$ to $\mathcal{B}$, and if there is (V_2, h_2) in list L_2, $\mathcal{B}$ returns h_2 to $\mathcal{A}$. Otherwise, $\mathcal{B}$ randomly selects $h_2 \in \{0, 1\}^l$ to send $\mathcal{A}$ and adds (V_2, h_2) to the list L_2.
- H_3-queries: $\mathcal{B}$ creates a list L_3 (initially empty), $\mathcal{A}$ sends $V_3 \in \{0, 1\}^l$ to $\mathcal{B}$, and if (V_3, h_3) exists in list L_3, $\mathcal{B}$ returns h_3 to $\mathcal{A}$. Otherwise, $\mathcal{B}$ randomly selects $h_3 \in \{0, 1\}^l$ to send $\mathcal{A}$ and adds (V_3, h_3) to the list L_3.

Phase 2: $\mathcal{A}$ initiates the following queries to $\mathcal{B}$.

- O_{sk} : After receiving the attribute set S submitted by $\mathcal{A}$, $\mathcal{B}$ queries the list $L_{sk}(S, d)$. If there is a private key corresponding to the attribute S in the list L_{sk}, $\mathcal{B}$ sends it to $\mathcal{A}$.
- O_{tk} : After receiving the attribute set S submitted by $\mathcal{A}$, $\mathcal{B}$ first looks up the (i, ok, S) in the list L_{ok}, if it exists, returns tk to $\mathcal{A}$. Otherwise, $\mathcal{B}$ performs the following three steps.
  1) If $i \neq i^*$ or $S \notin \Lambda^*$, $\mathcal{B}$ first obtains the corresponding private key d through O_{sk}, and then obtains the corresponding outsourced decryption key $ok = (tk, rk) = ((\hat{D}^{\eta}, \{(D_i^{\eta}, F_i^{\eta}) | i \in [1, n]\}), \eta)$ through the phase of outsourced decryption.
  2) If $i = i^*$ and $S \in \Lambda^*$, $\mathcal{B}$ obtains the corresponding private key d through O_{sk}, and then uses d to calculate

$ok = (tk, rk) = ((\mathbf{A}^{\varphi - r}, \{\mathbf{A}^{r_i/t_i} | i \in S\}, \{\mathbf{A}^{r_i/t_{n+i}} | i \notin S\}, \{\mathbf{A}^{r_i/t_{2n+i}} | i \in [1, n]\}, *)$, where $\{r_i | i \in [1, n]\}$ and r are random elements used to generate the corresponding private key d, and $*$ indicates that rk is unknown. That is, $\mathcal{B}$ sets $\eta = a$ when $i = i^*$ and $S \in \Lambda^*$.

3) $\mathcal{B}$ records (i, ok, S) in list L_{ok} and sends tk to $\mathcal{A}$.

- O_{rk} : Similar to O_{tk}, the only difference is that $\mathcal{B}$ sends retrieval key rk to $\mathcal{A}$.
- O_{od} : After receiving the (C_i, S, i) sent by $\mathcal{A}$, $\mathcal{B}$ first checks if S satisfies the access structure Λ corresponding to C_i. If not, output $\perp$; otherwise, $\mathcal{B}$ sends (tk, C_i) to $\mathcal{A}$.
- O_{dec} : After receiving the (C_i, S, i) sent by $\mathcal{A}$, $\mathcal{B}$ first checks if S satisfies C_i and the corresponding access structure Λ^*. If not, $\mathcal{B}$ outputs $\perp$; otherwise, $\mathcal{B}$ performs the following two steps.
  1) If $i \neq i^*$ or $S \notin \Lambda^*$, $\mathcal{B}$ uses rk to calculate m, and sends m to $\mathcal{A}$.
  2) If $i \neq i^*$ and $S \in \Lambda^*$, it can be found that the pairs $(V_1, h_1), (V_2, h_2), (V_3, h_3)$ in list L_1, L_2, L_3. Verify whether these tuples satisfy $V_1 = \zeta \parallel m$, $\bar{C}_1 = \zeta \oplus h_2$, $V_2 = \phi^{h_1}$, $\bar{C}_2 = m \oplus h_3$, and $V_3 = \zeta$. If not, $\mathcal{B}$ outputs $\perp$, otherwise checks whether $\bar{C}_5 = \hat{e}(\mathbf{A}, g)^{\varphi \cdot h_1}$ holds. If it does not, outputs $\perp$; otherwise, $\mathcal{B}$ sends m to $\mathcal{A}$.

Challenge: $\mathcal{A}$ selects two equal length plaintexts m_0^* and m_1^*, $\mathcal{B}$ sets $\bar{C}_1 = \zeta \oplus H_2(\mathbf{B}^{\varphi})$, $\bar{C}_2 = m_\theta \oplus H_3(\zeta)$, and $\bar{C}_3 = \mathbf{Z}^{\varphi}$, where $\zeta \in \{0, 1\}^l$. If $\mathbf{Z} = \hat{e}(g, g)^{abc}$ is true, the challenge ciphertext is valid.

Guess: $\mathcal{A}$ outputs guess result θ'. If $\theta = \theta'$, then $\hat{e}(g, g)^{abc} = \mathbf{Z}$, CT is a valid ciphertext; otherwise, CT is an invalid ciphertext.

$\mathcal{B}$ uses the above simulation to solve the MDDH problem, but the MDDH problem is difficult. Therefore, the probability of attack is negligible; that is, our scheme meets the requirement for confidentiality.

2) UNFORGEABILITY

According to the analysis results of [11], we suppose that the signature $\sigma = (\sigma_0, \sigma_1, \sigma_2)$ is valid for the medical data. In our scheme, the ABS protocol ensures that the medical data cannot be forged. Only the users who meet the access control policies formulated by the patient can calculate the signature of the medical data. It is impossible for a user who does not have the corresponding attribute i to compute $\hat{e}(g^{\alpha_{\rho(M_k)}}, g)$ and $\hat{e}(H_4(GID)^{\gamma_{\rho(M_k)}}, g^{\tau_k})$. Since $\tau_k \in Z_p$ is randomly chosen by the user, the signature σ cannot be forged.

3) ANONYMITY

The AAO assigns corresponding attributes to all of the entities in the system, which are bound to the global identity identifier *GID*. When other users in the system check the correctness of the signature, only the attribute verification key associated with the signature can be successfully checked. That is to say, when the data user looks over the medical data, they can verify that the medical data were established by a legitimate user without revealing the user's true identity. Therefore, our scheme can achieve the requisite anonymity.

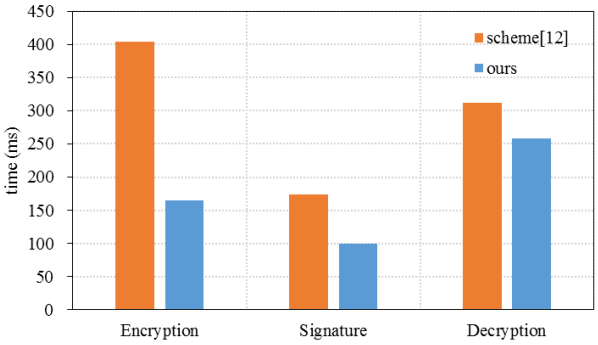

FIGURE 2. Comparison of time in each stage.

TABLE 1. Comparison of calculation costs.

Algorithm	Data encryption	Data decryption
[12]	$P + (3n+1)E + E_T$	$(2n+1)P + E_T$
Ours	$(n+2)E + E_T$	$P + E_Z + 2E_T$

B. PERFORMANCE ANALYSIS

In this section, we analyze and compare the computation cost between our scheme and that of Wang and Song [12]. The experimental environment is on a Windows 10 (64-bit) operating system with an Intel Core i5 3GHz processor with 8 GB RAM. The encoding is implemented by using the JPBC 2.0 library. The notations used in this section are defined as follows:

Notation	Description
E	the exponential operations in group G
E_T	the exponential operations in group G_T
E_Z	the exponential operations in ring E_P
P	the pairing operations

As can be seen in Table 1, the calculation cost of encryption and decryption operations in our scheme is significantly lower than that of Wang and Song [12]. In the phase of medical data encryption, our scheme needs $(n + 2)E + E_T$ operations. However, scheme [12] costs $P + (3n + 1)E + E_T$ operations, which increases the pairing and the exponential operations in group G. During the medical data decryption stage, our scheme outsources the medical data ciphertext to the CSP for partial decryption, which only needs $P+E_Z+2E_T$ operations. But $(2n+1)P+E_T$ of computation cost is required by the data users to decrypt the medical data ciphertext in [12]. Hence, the computational overhead of our scheme is greatly reduced compared with [12].

As shown in Fig. 2, compared with scheme [12], our scheme has lower computational overhead in the stages of encryption, signature, and decryption.

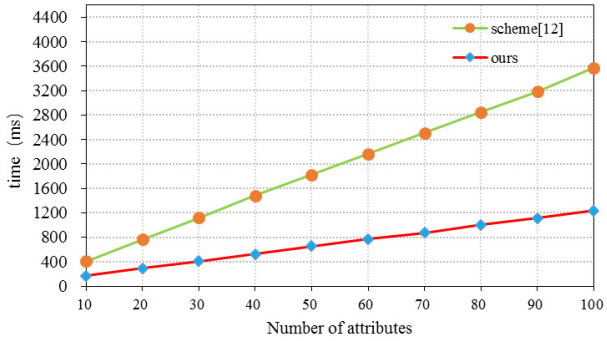

FIGURE 3. Encryption time.

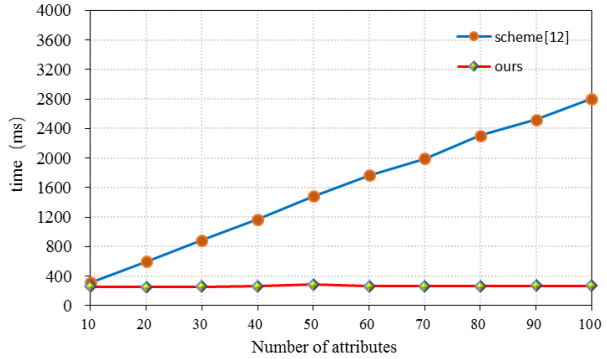

FIGURE 4. Decryption time.

As illustrated in Fig. 3, the time cost between scheme [12] and our scheme in the encryption phase is positively correlated with the number of attributes, but the time cost in [12] is always higher than our scheme.

Fig. 4 shows that there is a linear growth trend on the decryption phase of Wang and Song [12], while the number of attributes increases. The decryption time cost of our scheme remains basically unchanged as the number of attributes grows, since the most complex decryption work is delegated to the CSP. In summary, the proposed scheme has high computational performance.

VII. CONCLUSION

This paper proposes a new medical data sharing scheme that combines the advantages of cloud storage and blockchain technology. Our scheme uses the cloud server to store encrypted medical data, and the blockchain system to preserve the address of corresponding medical data ciphertext and medical-related information. Therefore, the proposed scheme satisfies the requirements for immutability and unforgeability. By using the attribute-based cryptosystem, the confidentiality of medical data in the cloud can be ensured, and the authenticity of the medical data source can be verified. Furthermore, the computational burden of medical data users can be alleviated through the use of the OD-ABE mechanism. The analysis results show that the proposed scheme has high performance in both computation overhead and security.

REFERENCES

[1] T. Schabetsberger, E. Ammenwerth, S. Andreatta, G. Gratl, R. Haux, G. Lechleitner, K. Schindelwig, C. Stark, R. Vogl, I. Wilhelmy, and F. Wozak, "From a paper-based transmission of discharge summaries to electronic communication in health care regions," *Int. J. Med. Inform.*, vol. 75, nos. 3–4, pp. 209–215, Mar. 2006.

[2] H. Cheng, C. Rong, K. Hwang, W. Wang, and Y. Li, "Secure big data storage and sharing scheme for cloud tenants," *China Commun.*, vol. 12, no. 6, pp. 106–115, Jun. 2015.

[3] M. Shen, B. Ma, L. Zhu, R. Mijumbi, X. Du, and J. Hu, "Cloud-based approximate constrained shortest distance queries over encrypted graphs with privacy protection," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 4, pp. 940–953, Apr. 2018.

[4] F. Xhafa, J. Li, G. Zhao, J. Li, X. Chen, and D. S. Wong, "Designing cloud-based electronic health record system with attribute-based encryption," *Multimedia Tools Appl.*, vol. 74, no. 10, pp. 3441–3458, 2015.

[5] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[6] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, "A blockchain-based approach to health information exchange networks," in *Proc. NIST Workshop Blockchain Healthcare*, vol. 1, 2016, pp. 1–10.

[7] W. Liang, M. Tang, J. Long, X. Peng, J. Xu, and K.-C. Li, "A secure FaBric blockchain-based data transmission technique for industrial Internet-of-Things," *IEEE Trans Ind. Informat.*, vol. 15, no. 6, pp. 3582–3592, Jun. 2019.

[8] A. Ekblaw, "A case study for blockchain in healthcare: MedRec prototype for electronic health records and medical research data," in *Proc. Proc. IEEE Open Big Data Conf.*, 2016, p. 13.

[9] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30.

[10] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, "Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives," *Cryptography*, vol. 3, no. 1, pp. 3–19, Jan. 2019.

[11] Y. Sun, R. Zhang, X. Wang, K. Gao, and L. Liu, "A decentralizing attribute-based signature for healthcare blockchain," in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul./Aug. 2018, pp. 1–9.

[12] H. Wang and Y. Song, "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain," *J. Med. Syst.*, vol. 42, no. 8, pp. 152–161, Jul. 2018.

[13] C. Doukas, I. Maglogiannis, V. Koufi, F. Malamateniou, and G. Vassilacopoulos, "Enabling data protection through PKI encryption in IoT m-health devices," in *Proc. IEEE 12th Int. Conf. Bioinf. Bioeng. (BIBE)*, Nov. 2012, pp. 25–29.

[14] M. C. Mont, P. Bramhall, and K. Harrison, "A flexible role-based secure messaging service: Exploiting IBE technology for privacy in healthcare," in *Proc. 14th Int. Workshop Database Expert Syst. Appl. (DEXA)*, Prague, Czech Republic, 2003, pp. 432–437.

[15] 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 encryption," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, Jan. 2013.

[16] M. Abomhara and H. Yang, "Attribute-based authenticated access for secure sharing of healthcare records in collaborative environments," *Hospital*, vol. 3, no. 6, pp. 3–20, 2016.

[17] F. Zhao, T. Nishide, and K. Sakurai, "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems," in *Proc. 7th Int. Conf. Inf. Secur. Pract. Exper.*, Guangzhou, China, 2011, pp. 83–97.

[18] A. Shamir, "Identity-based cryptosystems and signature schemes," *Crypto*, vol. 84, pp. 47–53, Aug. 1984.

[19] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM J. Comput.*, vol. 32, no. 3, pp. 586–615, Jan. 2003.

[20] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. EUROCRYPT*, Aarhus, Denmark, 2005, pp. 457–473.

[21] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS)*, 2006, pp. 89–98.

[22] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS)*, 2007, pp. 195–203.

[23] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS)*, 2007, pp. 456–465.

[24] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in *Proc. ICALP*, 2008, pp. 579–591.
[25] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, vol. 2010, pp. 62–91.
[26] J. Cui, H. Zhou, H. Zhong, and Y. Xu, "AKSER: Attribute-based keyword search with efficient revocation in cloud computing," *Inf. Sci.*, vol. 423, pp. 343–352, Jan. 2018.
[27] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Trans. Dependable Secure Comput.*, to be published.
[28] P. Yang, Z. Cao, and X. Dong, "Fuzzy identity based signature," IACR Cryptol. EPrint Arch., Lyon, France, Tech. Rep. 2008/002, 2008, p. 2. [Online]. Available: http://eprint.iacr.org/2008/002
[29] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures: Achieving attribute-privacy and collusion-resistance," IACR Cryptol. EPrint Arch., Lyon, France, Tech. Rep., Apr. 2008. [Online]. Available: https://eprint.iacr.org/2008/328.pdf
[30] J. Li, M. H. Au, W. Susilo, D. Xie, and K. Ren, "Attribute-based signature and its applications," in *Proc. 5th ACM Symp. Inf., Comput. Commun. Secur. (ASIACCS)*, 2010, pp. 60–69.
[31] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Proc. 30th Annu. Int. Conf. Adv. Cryptol. (EUROCRYPT)*, vol. 2011, pp. 568–588.
[32] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," in *Proc. 20th Usenix Conf. Secur.*, 2011, p. 34.
[33] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 8, pp. 1343–1354, Aug. 2013.
[34] J. Li, X. Li, L. Wang, D. He, H. Ahmad, and X. Niu, "Fuzzy encryption in cloud computation: Efficient verifiable outsourced attribute-based encryption," *Soft Comput.*, vol. 22, no. 3, pp. 707–714, Feb. 2018.
[35] B. Qin, R. H. Deng, S. Liu, and S. Ma, "Attribute-based encryption with efficient verifiable outsourced decryption," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 7, pp. 1384–1393, Jul. 2015.
[36] X. Mao, J. Lai, Q. Mei, K. Chen, and J. Weng, "Generic and efficient constructions of attribute-based encryption with verifiable outsourced decryption," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 5, pp. 533–546, Sep./Oct. 2016.
[37] H. Ma, R. Zhang, Z. Wan, Y. Lu, and S. Lin, "Verifiable and exculpable outsourced attribute-based encryption for access control in cloud computing," *IEEE Trans. Dependable Secure Comput.*, vol. 14, no. 6, pp. 679–692, Nov. 2017.
[38] C. Zuo, J. Shao, G. Wei, M. Xie, and M. Ji, "CCA-secure ABE with outsourced decryption for fog computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 730–738, Jan. 2018.
[39] D. Boneh, I. Mironov, and V. Shoup, "A secure signature scheme from bilinear maps," in *Proc. CT-RSA*, 2003, pp. 98–110.
[40] A. Beimel, O. Farràs, Y. Mintz, and N. Peter, "Linear secret-sharing schemes for forbidden graph access structures," in *Proc. Theory Cryptogr. Conf.* Cham, Switzerland: Springer, 2017, pp. 394–423.
[41] H. Chabanne, D. H. Phan, and D. Pointcheval, "Public traceability in traitor tracing schemes," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2005, pp. 542–558.

XIAODONG YANG (Member, IEEE) received the B.S. degree in mathematics from Northwest Normal University, China, in 2002, the M.S. degree in cryptography from Tongji University, China, in 2005, and the Ph.D. degree in cryptography from Northwest Normal University, in 2010. He is currently a Postdoctoral Fellow with the State Key Laboratory of Cryptology, China, and a Professor of information and computer science with Northwest Normal University. His research interests include applied cryptography, network security, and cloud computing security. He is a member of the Chinese Cryptology and Information Security Association.

TING LI received the B.S. degree from Zhengzhou Normal University, Zhengzhou, China, in 2018. She is currently pursuing the master's degree in computer science with Northwest Normal University. Her current research interests include network security, and blockchain technology and their applications.

XIZHEN PEI received the B.S. degree from Shanxi Datong University, Datong, China, in 2018. She is currently pursuing the master's degree in computer science with Northwest Normal University. Her current research interest includes cloud-computing security.

LONG WEN was born in Wuhan, Hubei, China, in 1996. He is currently pursuing the master's degree with the College of Computer Science and Engineering, Northwest Normal University, Lanzhou, China. His research interests include cryptology and information security.

CAIFEN WANG received the Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2003. She is currently a Professor of computer science with Shenzhen Technology University. Her current research interests include network security, cryptographic protocols, and security engineering. She is a member of the Chinese Cryptology and Information Security Association.