Hindawi
Security and Communication Networks
Volume 2019, Article ID 6782753, 10 pages
https://doi.org/10.1155/2019/6782753

Research Article

A Distributed Access Control with Outsourced Computation in Fog Computing

Qihua Wang[1,2] **Huaqun Wang**[3] **Yufeng Wang**[1] **and Rui Guo**[2]

[1]*School of Medical Information Engineering, Jining Medical University, Rizhao 276826, China*
[2]*Shanxi Key Laboratory of Information Communication Network and Security, Xian University of Posts & Telecommunications, Xian, 710121, China*
[3]*Jiangsu Key Laboratory of Big Data Security & Intelligent Processing, College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210023, China*

Correspondence should be addressed to Qihua Wang; wd19791209@163.com

Received 14 March 2019; Revised 3 June 2019; Accepted 18 June 2019; Published 8 July 2019

Academic Editor: Prosanta Gope

With the rapid development of information technology and the Internet of Things Technology (IOT), data security and healthy privacy are getting a lot of attention. In order to store, access, and share electronic health records, storage of this data is transferred to a third-party-cloud server. The security and privacy of electronic health records stored at date center or cloud server are not guaranteed. Before being sent to date center or cloud server, this data should be encrypted. Designing an efficient and secure fine-grained access control strategy for personal health records is facing enormous challenges. Security and privacy for electronic health records are very important because the electronic health data which plays an important role in medical server and treatment is directly associated with a particular patient. Attribute-based encryption (ABE) can effectively achieve fine-grained access control. However, the computation of bilinear pairings requires a large amount of computation overhead in ABE scheme. In order to decrease the computational overhead and ensure the confidentiality of electronic health records, a distributed fine-grained access control scheme with outsourced computation for IOT is proposed in this paper. Little calculation is executed by the receiver and sender in our proposed scheme. Outsourcing computing reduces the computing burden. The analyses of safety and performance show that our proposed scheme is safe and effective compared with previous schemes.

1. Introduction

With the development of cloud computing and IOT in several years, electronic health information systems provide real-time, fast, and effective services between patients and healthcare organizations. To cut down the burden of the terminal smart device, the patient outsources his/her e-health records to cloud service provider. Terminal devices or cloud servers are not completely trusted by data owners or patients. Security and privacy for electronic health data is very important because the electronic health data is directly associated with a particular patient, which plays an important role in medical server and treatment.

Fog computing which works between cloud computing and terminal devices can solve the bottleneck problem of data storage and data transmission in a certain extent [1, 2]. It can provide many services such as outsourced computing, network routing, and data storage. As shown from Figure 1, terminal equipment can communicate with fog device which can be attached to cloud service. With the rapid development of mobile internet, as shown from Figure 2 we can see that people are becoming more and more dependent on cloud service platform. The number of intelligent terminal device in the network is increasing greatly. It will not only occupy a large number of network bandwidth but also increase the burden of cloud server or data center and network latency. Data acquisition and data transmission are greatly affected. Therefore, in the cloud computing or fog computing environment, how to design an efficient and secure access control scheme still faces a challenge [3, 4]. Compared

to the traditional data access control scheme, the system model and the network structure in the fog computing environment are different. Fog device can provide users with computing, transmission, and storage services, so the cost of communication and computation is less for users. Therefore, the new access control scheme should be considered in IOT environment for users.

Attribute-based encryption (ABE) can be widely used in fine-grained access strategy for data storage in cloud environment [5–7]. The computation cost for ABE is large, and the computation cost linearly increases with the number of attributes in access control structure. Therefore, ABE is not suitable for the mobile terminals with limited power resources. Literature [8] first proposed the attribute-based encryption in multiauthority scheme. In literature [9], a distributed authorization scheme was proposed for wireless sensor nodes, but the authors did not consider the power resources of the sensor nodes. Outsourced computing can reduce the computing cost in the encryption and decryption phase [10–12]. Single authorized institution has problems of security risks and scale expansion. Literature [13], a fast encryption scheme for multiauthority scheme was proposed.

An attribute-based encryption scheme is proposed for multiuser environment based on personal health records system in literature [14]. Compared with previous similar works, this scheme had higher computing performance and security. Liu et al. [15] addressed an effective attribute-based signature scheme with fine-grained access control strategy in cloud data center for personal health records. Hu et al. [16] designed a fuzzy attribute-based signature strategy for wireless body area networks (WBAN). It can protect patients' privacy and support emergency personnel to access encrypted information. This scheme has strong practical value. To solve the privacy of the patients, Zhang et al. [17] proposed a secure smart health system. In this system, data owner can securely share data to resistance the leakage attacks. Rao et al. [18] also proposed a ciphertext policy attribute-based signcryption mechanism for personal health management system. This mechanism can simultaneously achieve confidentiality, privacy protection, public verifiability and fine-grained access control.

In ABE mechanism, the length of ciphertext or the number of bilinear pairs grows with the number of attributes. To deal with this problem, ABE schemes which had constant ciphertext length were addressed in literature [19–21]. In order to guarantee the privacy and security of medical health data, Wang et al. [22] proposed an efficient pairing-based fair remote retrieval scheme for outsourced private medical health data. In order to protect the content of e-health records for medical information records, some authors [23] proposed the idea of multiauthority content-based encryption mechanism to ensure the privacy of the patients. The article [24] gave a comprehensive overview of health data between searchable encryption and outsourcing computing services. To ensure the privacy of patients, access control policies IOT-based were proposed [25, 26]. Fan et al. [27] proposed a multiauthority mechanism in fog computing and cloud data center. Data owners and users can encrypt and decrypt data

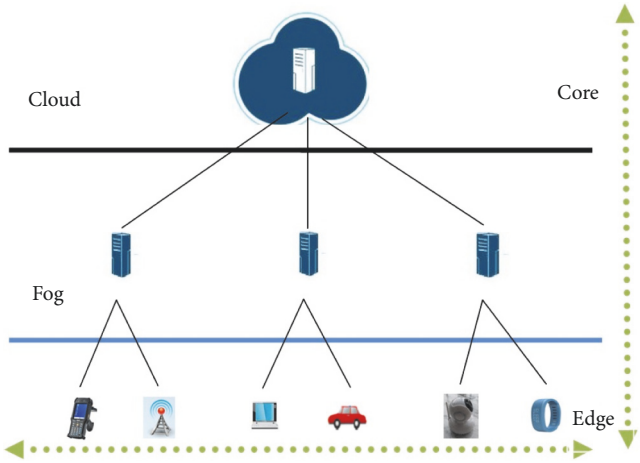

Figure 1: Fog computing architecture.

with only a small amount of computation. The authorized institutions in this scheme are independent of each other, and there is no information interaction among them. Based on literature [9, 27], we propose a distributed fine-grained access control scheme with outsourced computation in fog computing for electronic health records. Gope et al. [28] proposed a new secure communication architecture for fog computing. The authors introduced an extended concept of fog computing. Edge device and fog device were regarded as extensive fog computing layer. Moreover, the scheme in literature [28] can reduce the communication cost. The proposed scheme in literature [28] is suitable for resource-limited IOT device because they use lightweight cryptographic operations, such as one-way hash function and xor operations.

The proposed scheme is similar to the work of Ruj et al. [9]. However, our scheme is different from that of Ruj et al. in the following aspects. Firstly, Outsourcing encryption and outsourcing decryption strategies are not used in literature [9]. Secondly, distributed access control was used for wireless sensor network in literature [9], but they did not consider the computing ability of the sensor node, and our distributed authority is used in fog computing in this work. The main intention of our encryption scheme is to reduce to computational burden and guarantee the data confidentiality and security.

The remaining section of this work is organized as follows. Section 2 provides the related cryptology backgrounds of this work. Section 3 describes construction of our proposed scheme. Section 4 gives the analysis of security and performance for the proposed scheme. Finally, Section 5 concludes this work.

2. Cryptographic Backgrounds

In this part, some cryptographic backgrounds used in this paper are listed as follows.

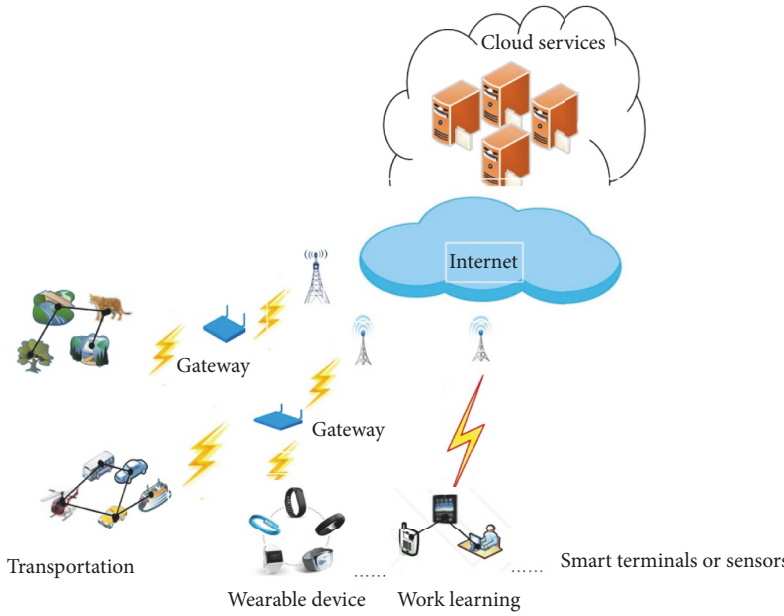

Figure 2: IoT architecture.

2.1. Bilinear Maps. Let G_o and G_1 be two cyclic groups of prime order p. Let g be a generator of G_o. A bilinear map $e : G_o \times G_o \longrightarrow G_1$ with the following property.

(1) Bilinearity. $\forall R, S \in G_o$ and $a, b \in Z_p$; we have $e(R^a, S^b) = e(R, S)^{ab}$.

(2) Nondegeneracy. $\exists R, S \in G_o$, such that $e(R, S) \neq 1$.

(3) Computability. $\forall R, S \in G_o$; there is an efficient algorithm to calculate $e(R, S) = 1$.

2.2. Key-Policy Attribute-Based Encryption. Key-policy ABE (KP-ABE) was proposed by Goyal et al. in literature [29]. In this subsection, we reviewed the KP-ABE scheme. KP-ABE scheme mainly consists of the following four algorithms.

(1) Setup (1^k). This algorithm outputs the public key PK and the system master secret key MK. The security parameter k is used as input parameter

(2) Encryption(m, γ, PK). The message m, public key PK, and the set of attributes γ are used as input parameters. This algorithm outputs the ciphertext E.

(3) Key Generation(P, MK). The access control structure, master secret key, and public key are used as input parameters. This algorithm outputs the secret key SK if the set of attributes matches the access control structure.

(4) Decryption(E, SK). The private key SK and ciphertext E are used as input parameters. This algorithm outputs the message m if the set of attributes matches the access control structure P.

3. System Model and Access Control Construction

In this part, system model and security model of the proposed scheme are described in detail.

3.1. System Model. The system model of our proposed scheme consists of six entities: data owner, data center, fog device, distribute authority (DA), data user, and authority center (AC), as shown in Figure 3.

The system model of our proposed scheme consists of six entities: data owner (patient), data center, fog device, distribute authority (DA), data user, and authority center (AC), as shown in Figure 3.

(1) Data Owner. In Figure 3 data owner is also called patient in our scheme. The data owner can use the mobile terminal to communicate with the fog device and outsources the message to the fog device. Power resources and computing ability of the mobile device is limited, but it has enough storage space. All data owned by data owner can be stored in the data center.

(2) Data Center. Data center provides data access control services, which is honest and curious. That is to say, data center is semitrusted. It can store huge amounts of data and has powerful computing power and electricity. It belongs to centralized cloud computing.

(3) Fog Device. It is responsible for data transmission and temporary storage. It is also responsible for the encryption and decryption data. The fog device encrypts the data partially and then sends the ciphertext to data center. The fog device can decrypt the data partially and send it to the legitimate users. Fog device is semitrusted. It provides data

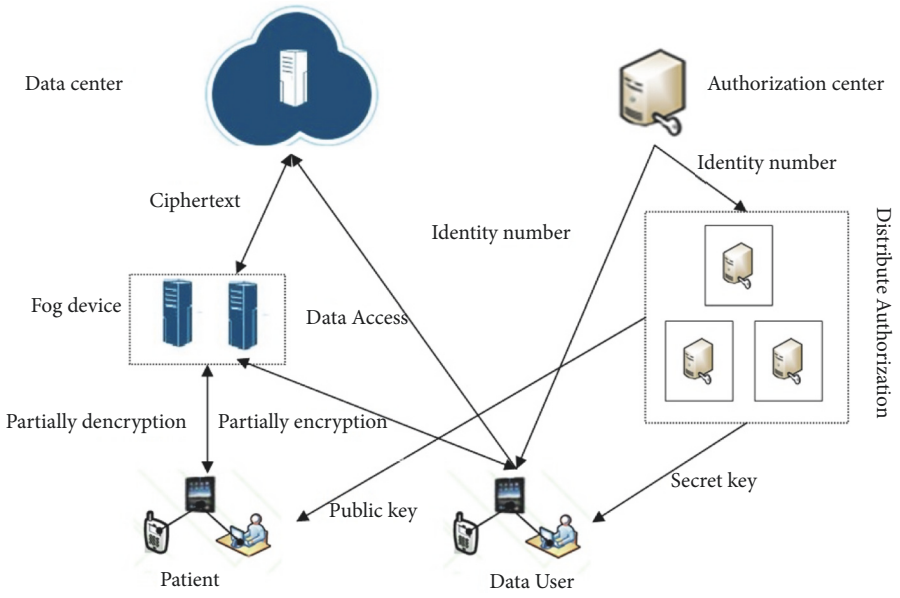

Figure 3: System model of the proposed scheme.

storage, data processing, and other network services between mobile device and traditional cloud data center.

(4) Distribute Authority. The distribute authority is fully trusted. It can independently manage each type of attribute. The distribute authority jointly generates the private key for legitimate users. In addition, a single authority cannot extract the user's private key. Each distributed authorization center has fixed attributes.

(5) Data User. The data user is equipped with smart device which is attached to fog devices. It can obtain its private key from DA. If the access structure of data user satisfies attribute sets of the ciphertext, fog device can partially decrypts ciphertext with the conversion key. Once receiving the partially decryption ciphertext from the fog device, the data user can obtain symmetric key with its secret key, and then it can decrypt the ciphertext using symmetric key.

(6) Authority Center. It is responsible for publishing the identity of each distributed authorization center and each user. Authority center assigns access control structures for each user.

3.2. System Definition. Eight algorithms in the proposed scheme are described as follows.

(1) System Setup (A). System setup algorithm is performed by authority center (AC). The symbol A represents the set of attributes. The parameter A is used as input parameter. This algorithm has three outputs. They are the identity and attribute owned by each distributed authority (DA), the identity of each fog device.

(2) Authority Setup (DA_{id}, k, A_{id}). Authority setup algorithm is performed by each DA. The symbols DA_{id}, k, A_{id} represent each distributed authority, security parameter, and attributes which are owned by each distributed authority DA_{id}, respectively. The identity and attribute of each distributed authority DA_{id} and security parameter are used as input parameters. This algorithm outputs the system global parameter P. In this paper, the attributes which are owned by each distributed authority satisfy the following equations:

$$A_{id1} \bigcap A_{id2} \bigcap \cdots \bigcap A_{idn} = \text{ø} \quad (1)$$

$$A_{id1} \bigcup A_{id2} \bigcup \cdots \bigcup A_{idn} = A \quad (2)$$

(3) Keygen-FD (FD_{id}). Keygen-FD algorithm is run by fog device (FD). The symbol FD_{id} represents the identity of FD. It is used as input parameter. This algorithm outputs public key and secret key for FD.

(4) Encrypt-Owner (M, K). Encrypt-owner algorithm is run by data owner (DO). Message M and symmetric key K are used as input parameters. This algorithm outputs symmetrically encrypted ciphertext CT.

(5) Encrypt-Out (SP, CT, DO_i). Encrypt-Out algorithm is performed by FD. The symbol DO_i represents attributes of DO. The public parameter SP, symmetrically encrypted ciphertext CT and DO_i are used as input parameters. This algorithm outputs the final ciphertext CT'.

(6) Keygen-User (SP, T_i). Keygen-User algorithm is performed by each DA. The public parameter SP and access control structure T_i of the data user are used as input parameters. This algorithm outputs the private key for data user.

(7) Decrypt-Out (CT'). Decrypt-Out algorithm is run by FD. The final ciphertext is used as input parameter CT'. This

algorithm outputs the symmetrically encrypted ciphertext CT.

(8) Decrypt-User (CT). Decrypt-User algorithm is run by data user. The symmetrically encrypted ciphertext CT is used as input parameter. This algorithm outputs the message M.

3.3. Access Control Construction. In this section, the access control construction of this paper is given. Compared to literature [9], the main difference is that the distributed outsourcing encryption and decryption are used for electronic health record environment in fog computing. In order to make this work more complete, detailed description of the proposed scheme is given as follows.

3.3.1. System Setup

(1) AC Initialization. Authority center distributes identity information for each entity, and it chooses a hash function.

$$h : \{0,1\}^* \longrightarrow G_0^* \tag{3}$$

In this work, the hash function is denoted by $h(.)$.

(2) DA Initialization. (1) DA executes the corresponding algorithm and outputs the global parameter $GP = \{p, e, G_0, G_1, g\}$.

(2) In this work, the set of DA is denoted by Q. Each distribute authority DA_i $(i \in Q)$ randomly chooses a number $\rho_i \in Z_q^*$ and computes $Y_i = e(g,g)^{\rho_i}$. The result of calculation is sent to all distribute authorities. The following information can be obtained by each distribute authority.

$$Y = \prod_{i=1}^{i=n} Y_i = e(g,g) \prod_{i=1}^{i=n} \rho_i \tag{4}$$

(3) For any two distribute authorities $< i, m >, i \neq m$, they can share the data $\sigma_{im} = \sigma_{mi} \in Z_q^*$ with each other, but any other distribute authority cannot obtain the number σ_{im}. For all distribute authorities, the following symmetric matrix σ can be obtained. The data element σ_{mm} of the main diagonal in symmetric matrix is ∞.

$$\sigma = \begin{bmatrix} \sigma_{11} & \sigma_{12} & \cdots & \sigma_{1n} \\ \sigma_{21} & \sigma_{22} & \cdots & \sigma_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_{n1} & \sigma_{n2} & \cdots & \sigma_{nm} \end{bmatrix} \tag{5}$$

(4) Each DA_i $(i \in Q)$ randomly chooses a number $x_i \in Z_q^*$ and computes $y_i = g^{x_i}$, The message y_i is broadcast to others. For a user u_j, DA_i and DA_m can compute the following message.

$$F_{im}(j) = g^{x_i x_m / \sigma_{im+j}} \tag{6}$$

The DA_i and DA_m share the same number σ_{im}, so they can obtain $F_{im}(j)$ for a user u_j.

(5) The DA_i $(i \in Q)$ picks for each attribute $a \in L_i$ owned by device DA_i, a random number $t_{a,i} \in Z_q^*$, and calculates $T_{a,i} = g^{t_{a,j}}$. The symbol L_i denotes the set of attributes that DA_i possesses. The private key of fog device DA_i $(i \in Q)$ is $< x_i, \{\sigma_{im}\}_{m \in Q \setminus i}, \{t_{a,i}\}_{a \in L_i} >$.

The public parameters of the whole system are $< Y = e(g,g)^{\sum_{i=1}^{i=Q} \rho_i}, (y_i, \{T_{a,i} = g^{t_{a,i}}\}_{a \in L_j})_{i \in Q} >$.

In the above initialization (1)-(5), the fog device randomly selects four parameters $< \rho_i, x_i, t_{a,i}, r >$.

3.3.2. Key Generation. The private key of the user u_j (the receiver of the data or decipher of the data) can be calculated by DA_i $(i \in Q)$ as follows:

(1) Each DA_i $(i \in Q)$ randomly chooses a number $R[j]_{im} \in Z_q^* (m \in Q \setminus i)$. When i is equal to m, $R[j]_{im}$ is zero. For all devices, the following two matrices can be determined.

$$R = \begin{bmatrix} 0 & R_{12} & \cdots & R_{1n} \\ R_{21} & 0 & \cdots & R_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ R_{n1} & R_{n2} & \cdots & 0 \end{bmatrix}$$
$$D = \begin{bmatrix} 1 & D_{12} & \cdots & D_{1n} \\ D_{21} & 1 & \cdots & D_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ D_{n1} & D_{n2} & \cdots & 1 \end{bmatrix} \tag{7}$$

where

$$D_{im} = \begin{cases} g^{R[j]_{im}} F_{im}(j) & \text{if } i > m \\ 1 & \text{if } i = m \\ \dfrac{g^{R[j]_{im}}}{F_{im}(j)} & \text{if } i < m \end{cases} \tag{8}$$

(2) DA_i $(i \in Q)$ randomly selects a degree $d_i - 1$ polynomial $p[j](x)$ according to the access control structure owned by user. when x is equal to 0 we can obtain the following equation.

$$p[j](0) = \rho_i - \sum_{m=1}^{n} R[j]_{im} \tag{9}$$

The value of d_i is related to access control structure of the data user. d_i can be calculated in the following way:

$$d_i = \begin{cases} 1 & \text{see Figure 4} \\ I_j & \text{see Figure 5} \\ x & \text{see Figure 6} \end{cases} \tag{10}$$

where I_j denotes all the attributes owned by the user (see Figures 4, 5, and 6).

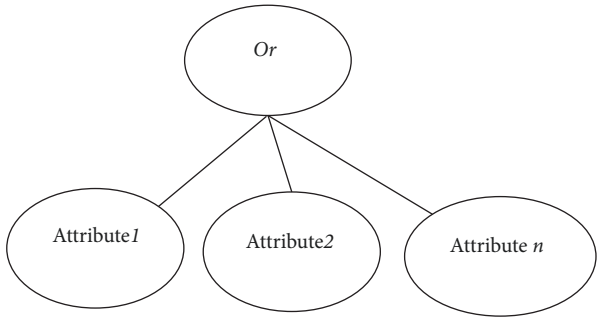

Figure 4: Access control structure of the user (or).

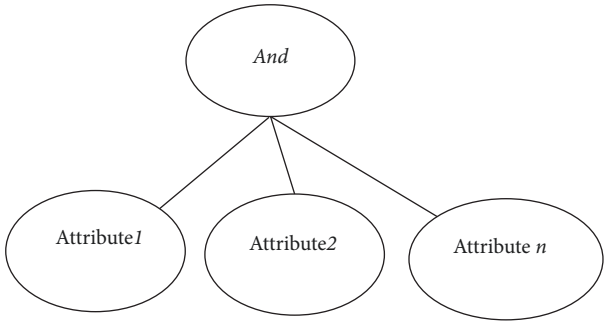

Figure 5: Access control structure of the user (and).

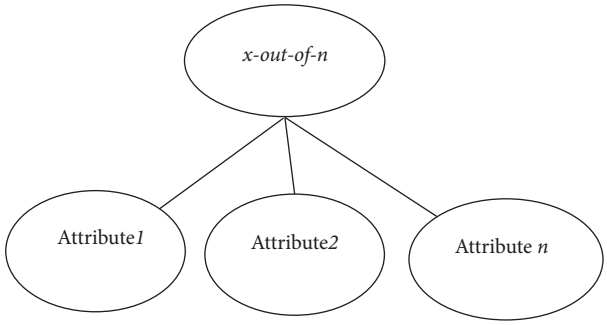

Figure 6: Access control structure of the user (x-out-of-n).

(3) Each DA_i $(i \in Q)$ calculates the secret key and sends it to the user u_j.

$$SK_{a,i} = g^{p[j]_i(a)/t_{a,j}} \tag{11}$$

(4) According to (1)-(3), the following expression D_j can be obtained by the mutual cooperation of DA_i $(i \in Q)$.

$$D_j = \prod D_{im} = g^{\sum R[j]_{im}} \tag{12}$$

3.3.3. The Generation of Public and Private Key for Fog Device. Fog device randomly chooses a number r. The public key and private key can be calculated in the following way.

$$\begin{aligned} PK_{DA_i} &= h\left(DA_i\right)^r, \\ SK_{DC_i} &= r \end{aligned} \tag{13}$$

Before the user sends the information, the user requests the attributes registration in the fog device. After the successful registration, the user randomly chooses a number α and computes K_S.

$$K_S = e\left((g)^{\alpha}, h\left(DA_i\right)^r\right) \tag{14}$$

3.3.4. Master Key Encryption and Message Encryption. The task to be completed at this stage is that the data sender (data owner) sends the ciphertext C_j' to fog device based on its owned attributes, public parameters, and message. The fog device encrypts the data based on KP-ABE.

(1) Data owner randomly selects a number $K \in Z_q^*$. The message M is encrypted using the symmetric key K by data owner.

(2) Data owner sends the symmetric encrypted ciphertext $C_j' = \{\{M\}_K, KK_S\}$ to fog device. The symbol $\{M\}_K$ denotes the symmetric encrypted ciphertext. Fog device can reencrypt the data and obtain the following ciphertext.

$$\begin{aligned} C_j = \Big\{ & L_a, \left\{E_{a,k} = T_{a,k}^r\right\}_{a \in I_a, k \in Q}, \ E' \\ & = g^r, g^{\alpha}, KK_s Y^r, \{M\}_K \Big\} \end{aligned} \tag{15}$$

3.3.5. Decryption. Authorized data user whose access control structure satisfies the attribute requirement in ciphertext can decrypt ciphertext.

The data user u_j requests for data access to data center. If the data user is an authorized user, he/she can obtain ciphertext C_j from data center. The authorized user can decrypt the ciphertext using secret key in traditional decryption scheme. The decryption process requires a lot of computational energy consumption. The computing power of users is limited, so authorized users can request outsourcing decryption. In our scheme, fog device can solve this problem. Fog device can obtain corresponding ciphertext from data center. The fog device can partially encrypt the ciphertext using conversion key of data user. The detailed process is as follows.

(1) The data user randomly chooses a numerical value $\tau \in Z_q^*$. The conversion key $(SK_{a,i})^{\tau}$ is sent to fog device by data user. For each attribute a, FD can compute F_i as follows.

$$F_i = e\left(E_{a,i}, SK_{a,i}{}^{\tau}\right) = \begin{cases} e\left(g,g\right)^{\tau r p[j]_i(a)} & \text{if a} \in I_i \\ \perp & otherwise \end{cases} \tag{16}$$

(2) If the number of attributes is d_i, FD can compute F_i according to Lagrange interpolation theorem [30].

$$\begin{aligned} F_i &= e\left(E_{a,i}, SK_{a,i}{}^{\tau}\right) = e\left(g,g\right)^{\tau r p[j]_i(a)} \\ &= e\left(g,g\right)^{\tau r\left(\rho_i - \sum_{m=1}^{Q} R[j]_{im}\right)} \end{aligned} \tag{17}$$

(1) Compute

$$Q = \prod_{i=1}^{i=Q} F_i \tag{18}$$

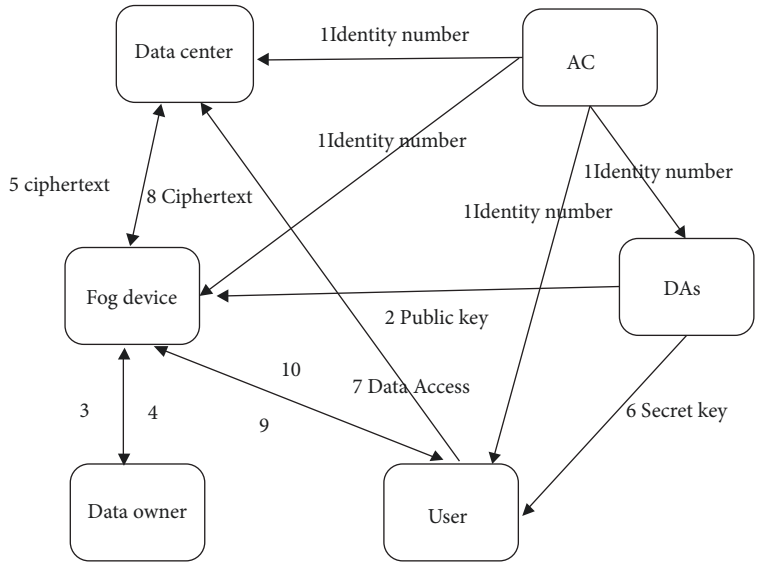

Figure 7: Work flow of our scheme.

(2) Compute

$$e\left(D_j, E'\right) Q = Y^{\tau r} \tag{19}$$

FD can obtain K_s.

$$K_s = e\left(g^{\alpha}, h\left(DA_i\right)^r\right) \tag{20}$$

FD can compute the partially ciphertext C_j' and send it to the user u_j.

$$C_j' = \left\{Y^{\tau r}, KK_s Y^r, e\left(g^{\alpha}, h\left(DA_i\right)^r\right)\right\} \tag{21}$$

(3) The symmetrical private key K is computed by the data user u_j. Finally, the data user decrypts $\{M\}_K$ using K.

$$K = \frac{KK_s Y^r}{e\left(g^{\alpha}, h\left(DA_i\right)^r\right)\left(Y^{r\tau}\right)^{1/\tau}} \tag{22}$$

In order to understand our proposed scheme clearly, we depict in detail the workflow of our solution in Figure 7. The workflow of our solution is outlined as follows.

(1) The authorization center is responsible for assigning identity information for data owner, fog device, data user, and distributed authority. It also distributes attribute set to each distributed authority.

(2) Distributed authorities work with each other. They produce the public parameters of the system.

(3) Data owner registers the owned attributes in fog device. The registration of attributes is prepared for the partial outsourced encryption.

(4) Data owner encrypts the original information by symmetric scheme. To guarantee the security of symmetric keydata owner can blind the symmetric key and then send the message to corresponding fog device.

(5) Fog device encrypts the message which is sent by data owner.

(6) DA sends the secret key to data user according to access control structure of the data user.

(7) If authorized user requests data access, she/he can decrypt the ciphertext in traditional scheme.

(8) Because computing power of the user is limited, the data center sends the ciphertext to the corresponding fog device.

(9) Data user sends the conversion key to fog device. Fog device can partly decrypt the ciphertext.

(10) Fog device sends the partly encrypted ciphertext to the user. Users can use less computation cost to obtain symmetrical secret key and obtain the original message.

4. Security Analysis and Performance Analysis

In this section, the security and performance analysis of our scheme are given.

4.1. Security Analysis. Each user has the unique identity information in the proposed scheme. The private key is issued by different DAs. In single authorized institution if the authority has been captured, the whole system will be paralyzed, and the private key will be leaked. Assume that there have been n authorized institutions in our scheme. Our proposed scheme is secure unless $n-1$ authorized institutions have been captured. Moreover, the users do not collude to obtain the original message.

Theorem 1. *Our distributed authorization scheme can ensure the correctness and privacy.*

Proof. In literature [31], the range of private keys is the finite field F_q. Assume that $\beta_1, \beta_2, \ldots, \beta_n \in F_q$ are n distinct nonzero values. All parties can know the values. In order to share the secret value $k \in F_q$, $t-1$ values $\beta_1, \beta_2, \ldots, \beta_{t-1}$ from F_q are randomly chosen. These randomly $t-1$ numbers and the secrets k can make up a randomly polynomial function

$f(x) = k + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$. The share of participant p_j is $z_i = f(\beta_i)$. The proof idea of correctness and privacy originates from literature [32]. For t distinct numbers $x_1, x_2, \ldots, x_t$, they denote t distinct parties and t numbers $y_1, y_2, \ldots, y_t$ denote the share of participant. There has been a unique polynomial f of degree $t-1$, such that $f(x_i) = y_i$ for each i $(1 \le i \le t)$.

(1) Correctness. There have been t points in set B for the polynomial function f. The polynomial function f can be reconstructed according to Lagrange's interpolation. We can compute $k = f(0)$. According to reconfiguration strategy, function $f(x)$ is calculated as follows.

$$f(x) = \sum_{l=1}^{t} z_{il} \prod_{1 \le j \le t, j \ne l} \frac{\beta_{ij} - x}{\beta_{ij} - \beta_{il}} \tag{23}$$

When knowing the polynomial function, the parties in set B can reconstruct the secret value k as follows.

$$f(0) = \sum_{l}^{t} z_{il} \prod_{1 \le j \le t, j \ne l} \frac{\beta_{ij}}{\beta_{ij} - \beta_{il}} = k \tag{24}$$

(2) Privacy. Any unauthorized set with $t-1$ parties has $t-1$ points for the polynomial function. According to possible share value $\tilde{z}_i$, a polynomial function with the degree $t-2$ can be restructured. According to the interpolation theorem, for set $\tilde{B} = \{p_{i1}, p_{i2}, \ldots, p_{i(t-1)}\}$ and any $\tilde{k} \in F_q$, there has been a unique polynomial function $\tilde{f}$ with the degree $t-1$. That is to say, $\tilde{f}(0) = \tilde{k}$ and $\tilde{f}(\beta_{il}) = \tilde{z}_{il} \ne f(\beta_{il}) = z_{il}, l \in [1, t-1]$. We can compute the following probability distribution.

$$\Pr\left[f(\beta_{il}) = z_{il},\ (1 \le l \le t-1) \mid k = \tilde{k}\right] = \frac{1}{q^{t-1}} \tag{25}$$

The above distribution probability is the same for all. The probability of their consistency can be negligible. The privacy of the private key can be followed. Theorem 1 is established no matter in single authority or the distributed authority. □

4.2. Performance Analysis. We analyze the performance of our scheme in this part and compare to literature [7, 9, 29]. In this work, we only list the computation cost of the data user and data owner for encryption and decryption phase. A lot of calculation is done by fog device. The computation cost accomplished by fog device is not listed.

To computer computation cost, we define the following notations. To improve the reading, the symbols and their explanations should be given in Table 1. The symbol l denotes the number of the attribute that the sender possesses. The symbols C_P, C_{sm}, and C_{Ex} denote the computing time of a bilinear pair, computing time of one scalar multiplication in G_0, and the computing time of exponentiation in G_1, respectively. The symbol t_h denotes the computing time of general hash function. The symbol t_s denotes the computing time of symmetric encryption operation. The value of d_i is related to access control structure of data user. The implementation environment for related operations is a mobile device with 2GB RAM, 16GB ROM, Android 4.4 operating system, 2.45G processor, and battery capacity 2800mA [33]. Computation cost for encryption and decryption are listed in Tables 2 and 3. The implementation results [33, 34] of the main operations are listed in Table 4.

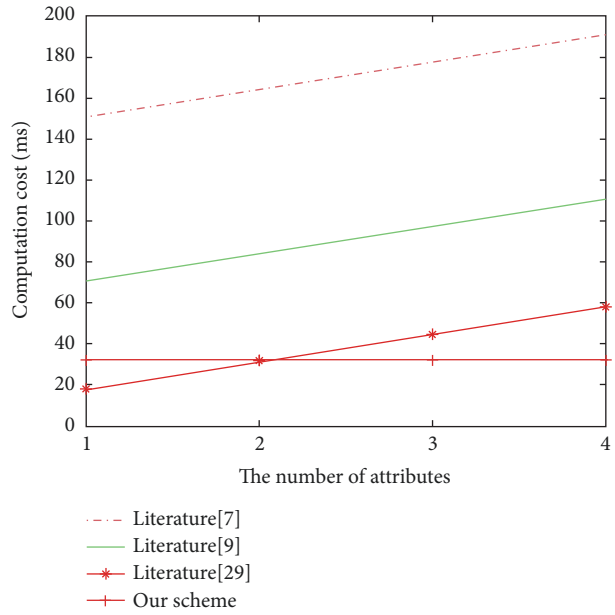

Figure 8: Comparison of computation cost in encryption.

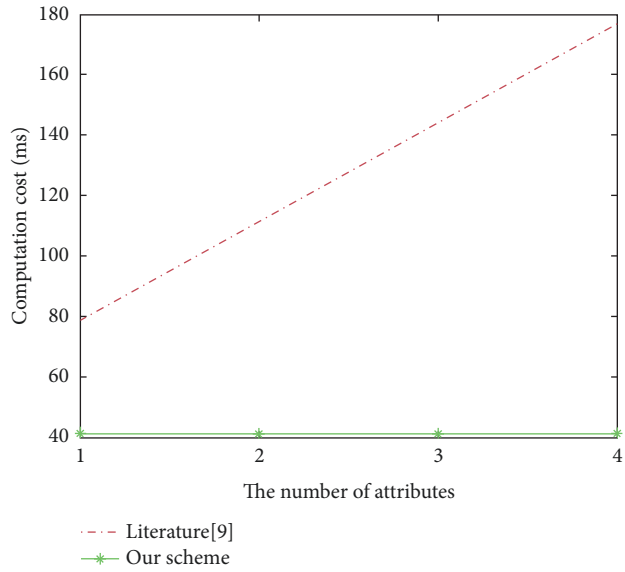

Figure 9: Comparison of computation cost in decryption.

Figures 8 and 9 show the comparison of encryption cost and decryption cost, respectively. When the value l equals 1 or 2, the encryption cost of our scheme is worse than that in scheme [2, 9]. The encryption cost of our scheme is better than that in scheme [7, 9]. Decryption cost is related to two parameters, so our scheme only compared to scheme [9] in Figure 9. As shown from Figures 8 and 9, the computation consumption for encryption operation and

Table 1: The meanings of main symbols.

The symbol	The meaning of each symbol
DA	The generic term of distribute authority
AC	Authority center
C_P	The computing time of a bilinear pair
C_{Sm}	The computing time of one scalar multiplication in G_0
C_{Ex}	The computing time of exponentiation computation in G_1
t_h	The computing time of general hash function
t_s	The computing time of symmetric encryption
l	The number of the attribute that the sender possesses
d_i	Related to the user's access control structure
DA_i	Each distribute authority
n	The number of distribute authority

Table 2: The encryption comparisons of computation cost.

Scheme	The cost of encryption
Literature [7]	$(l+5)C_{Sm} + 2C_{Ex} + 2C_P$
Literature [9]	$(l+2)C_{Sm} + t_h + t_s$
Literature [29]	$lC_{Sm} + 2C_{Ex}$
Our scheme	$t_s + C_P + t_h$

Table 3: The decryption comparisons of computation cost.

Scheme	The cost of decryption
Literature [7]	$4C_P + (3l+4)C_{sm} + C_{Ex}$
Literature [9]	$(d_i+1)C_P + C_{sm}$
Literature [29]	$lC_P + 2d_iC_{Ex}$
Our scheme	$3C_{Sm}$

Table 4: Computations cost of some operations.

Operations	*Computation cost (ms)*
C_P	32.713
C_{Sm}	13.401
t_h	0.006
t_s	0.001
C_{Ex}	2.249

decryption operation in the proposed scheme is constant. In our scheme, computation cost of the data user and data owner is independent of the number of attributes. The main reason is that many computation operations are executed by fog device. The computation consumption linearly increases with the number of attributes in literature [7, 9, 29]. Our scheme is more suitable for mobile terminal users with limited computing power and limited power consumption.

5. Conclusions

In this work, a distributed access control with outsourced encryption and decryption for electronic health records is introduced. The most computational cost of attribute-based encryption is performed by fog device. Our solution reduces computational effort of the sender and receiver. Our scheme can achieve fine-grained access control and guarantee the confidentiality of the message. The proposed scheme is more suitable for mobile terminal users with limited computing power and limited power consumption, such as smart phone and wireless sensor node. The analysis shows that our proposed scheme is safe and effective based on current computing technology. Our scheme is a practical and novel solution. It can also be extended to other application environments. When message is stored in data center, the proposed solution is necessary.

Data Availability

The data used in this study is available from references [33, 34].

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgments

The work is supported by Supporting Fund for Teachers' Research of Jining Medical University (No. JY2017KJ053 and No. JY2017KJ055), NSFC cultivation project of Jining Medical University (JYP2018KJ14), doctoral research fund of Jining Medical University (No. 600589002), National Natural Science Foundation of China (No. 61872192), Natural Science Foundation of Jiangsu Province (No. BK20181394), Qing Lan Project of Jiangsu Province, 1311 Talent Plan Foundation of NUPT, and Opening Project of Shaanxi Key Laboratory of Information Communication Network and Security (No. ICNS201806).

References

[1] A. Alrawais, A. Alhothaily, and C. Hu, "Fog computing for the internet of things: security and privacy issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34–42, 2017.

[2] K. Liang, L. Zhao, X. Chu, and H. Chen, "An integrated architecture for software defined and virtualized radio access

networks with fog computing," *IEEE Network*, vol. 31, no. 1, pp. 80–87, 2017.

[3] C. Esposito, A. Castiglione, F. Pop, and K. R. Choo, "Challenges of connecting edge and cloud computing: a security and forensic perspective," *IEEE Cloud Computing*, vol. 4, no. 2, pp. 13–17, 2017.

[4] M. A. Ferrag, L. A. Maglaras, H. Janicke et al., "Authentication protocols for internet of things: a comprehensive survey," *Security and Communication Networks*, vol. 2017, Article ID 6562953, 41 pages, 2017.

[5] Z. Wang, D. Huang, Y. Zhu, B. Li, and C. Chung, "Efficient attribute-based comparable data access control," *IEEE Transactions on Computers*, vol. 64, no. 12, pp. 3430–3443, 2015.

[6] H. Wang, Z. Zheng, L. Wu, and D. He, "New large-universe multi-authority ciphertext-policy ABE scheme and its application in cloud storage systems," *Journal of High Speed Networks*, vol. 22, no. 2, pp. 153–167, 2016.

[7] K. Liang and W. Susilo, "Searchable attribute-based mechanism with efficient data sharing for secure cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, pp. 1981–1992, 2015.

[8] M. Chase, "Multi-authority attribute based encryption," in *Theory of Cryptography*, pp. 515–534, Springer, Berlin, Germany, 2017.

[9] S. Ruj, A. Nayak, and I. Stojmenovic, "Distributed fine-grained access control in wireless sensor networks," in *Proceedings of the 25th IEEE International Parallel and Distributed Processing Symposium, IPDPS 2011*, pp. 352–362, Anchorage, Alaska, USA, May 2011.

[10] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertext," in *Proceedings of the Usenix Conference on Security*, pp. 34-34, 2011.

[11] H. Wang, D. He, and J. Han, "VOD-ADAC: anonymous distributed fine-grained access control protocol with verifiable outsourced decryption in public cloud," *IEEE Transactions on Services Computing*, 2017.

[12] H. Wang, D. He, J. Yu, and Z. Wang, "Incentive and unconditionally anonymous identity-based public provable data possession," *IEEE Transactions on Services Computing*, 2016.

[13] S. J. De and S. Ruj, "Decentralized access control on data in the cloud with fast encryption and outsourced decryption," in *Proceedings of the 58th IEEE Global Communications Conference, GLOBECOM 2015*, 6, 1 pages, USA, 2015.

[14] 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 Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2013.

[15] J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: ciphertext-policy attribute-based signcryption," *Future Generation Computer Systems*, vol. 52, pp. 67–76, 2015.

[16] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body area network security: a fuzzy attribute-based signcryption scheme," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 37–46, 2013.

[17] Y. Zhang, P. Lang, D. Zheng et al., "A secure and privacy-aware smart health system with secret key leakage resilience," *Security and Communication Networks*, vol. 2018, Article ID 7202598, 13 pages, 2018.

[18] Y. S. Rao, "A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing," *Future Generation Computer Systems*, vol. 67, pp. 133–151, 2017.

[19] C. Yanli, S. Lingling, and Y. Geng, "Attribute-based access control for multi-authority systems with constant size ciphertext in cloud computing," *China Communications*, vol. 13, no. 2, pp. 146–162, 2016.

[20] X. Li, S. Tang, L. Xu, H. Wang, and J. Chen, "Two-factor data access control with efficient revocation for multi-authority cloud storage systems," *IEEE Access*, vol. 5, no. 99, pp. 393–405, 2017.

[21] X. Mao, J. Lai, Q. Mei, K. Chen, and J. Weng, "Generic and efficient constructions of attribute-based encryption with verifiable outsourced decryption," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 5, pp. 533–546, 2016.

[22] H. Wang, Q. Wu, B. Qin, and J. Domingo-Ferrer, "FRR: Fair remote retrieval of outsourced private medical records in electronic health networks," *Journal of Biomedical Informatics*, vol. 50, pp. 226–233, 2014.

[23] R. Guo, X. Li, and D. Zheng, "Privacy-preserving medical information systems using multi-authority content-based encryption in cloud," in *Proceedings of the International Conference on Cloud Computing and Security*, Lecture Notes in Computer Science, pp. 268–279, 2017.

[24] R. Zhang, R. Xue, and L. Liu, "Searchable encryption for healthcare clouds: a survey," *IEEE Transactions on Services Computing*, vol. 11, no. 6, pp. 978–996, 2018.

[25] 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. 3, no. 1, pp. 1–15, 2018.

[26] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system," *Information Sciences*, vol. 479, pp. 567–592, 2019.

[27] K. Fan, J. Wang, X. Wang, H. Li, and Y. Yang, "A secure and verifiable outsourced access control scheme in fog-cloud computing," *Sensors*, vol. 17, no. 7, p. 1695, 2017.

[28] P. Gope, J. Lee, R. Hsu, and T. Q. Quek, "Anonymous communications for secure device-to-device-aided fog computing: architecture, challenges, and solutions," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 10–16, 2019.

[29] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*, pp. 89–98, November 2006.

[30] H. Wang, Y. Zhang, H. Xiong, and B. Qin, "Cryptanalysis and improvements of an anonymous multi-receiver identity-based encryption scheme," *IET Information Security*, vol. 6, no. 1, pp. 20–27, 2012.

[31] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[32] B. Amos, "Secret-sharing schemes: a survey," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, pp. 11–46, 2011.

[33] D. He, H. Wang, L. Wang, J. Shen, and X. Yang, "Efficient certificateless anonymous multi-receiver encryption scheme for mobile devices," *Soft Computing*, vol. 21, no. 22, pp. 6801–6810, 2017.

[34] F. G. Li and W. F. Wu, "Pairing-based cryptography," *Science Press*, pp. 18–42, 2014.