A Certificateless and Dynamic Conditional Proxy Re-encryption-based Data Sharing Scheme for IoT Cloud

Yousheng Zhou[1], Yurong Li[1], Yuanni Liu[2]*

[1] School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, China
[2] School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, China
zhouys@cqupt.edu.cn, s200201087@stu.cqupt.edu.cn, liuyn@cqupt.edu.cn

Abstract

The wide application of IoT Cloud makes the data security become a big concern for public. Although many secure data sharing schemes have been developed for Cloud data, most of them cannot fully meet the requirements of IoT Cloud, or fail to give consideration to efficiency on the premise of stable running under the resource-constrained IoT situations. In this paper, we propose a secure data sharing scheme that combines certificateless public key cryptography and proxy re-encryption to achieve multi-level data access control. Moreover, dynamic key update and ciphertext evolution are realized to effectively decrease the risk of key leakage. Quantitative performance analysis shows that the proposed scheme not only support privacy-preserving data sharing in IoT Cloud, but also has higher efficiency, and therefore it is more practical for IoT Cloud.

Keywords: IoT Cloud, Proxy re-encryption, Conditional re-encryption, Cloud sharing

1 Introduction

With the development of 5G communication technology, big data, Cloud computing and other next-generation network technologies, the Internet of Things (IoT) has gradually penetrated into various line of business. In the technical operation system, the Internet of Things, as the key task bearer for the collection and transmission of original data, manages and uses a huge number of IoT access devices, while generating and organizing massive data regarded as assets on the other. Cloud computing, supported by data acquired through the IoT, performs distributed storage and calculation of data, thus completing the transformation of data value. Therefore, for functional and economic reasons, a larger percentage of users tend to hand over their data to Cloud service providers which can storage and compute at lower cost. Hou et al. described the implementations for many servers with varying performance at great length, such as application servers, database cluster and brokers [1].

In view of the fact that Cloud Server Provider (CSP) is semi-trusted, it becomes particularly important to ensure the confidentiality, controllability and availability of Cloud data. In the past, the most effective method is for users to encrypt data before outsourcing, but the traditional encryption algorithm has many problems and deficiencies in IoT Cloud scenarios, in which case cannot meet user's requirements simultaneously. The data transmission between the data provider and the data consumer is confidential, and the CSP performing storage, forwarding and limited computing functions cannot obtain the data and secret keys. Different from other Cloud, IoT Cloud terminal devices typically do not have sufficient computing power to achieve comprehensive access control while ensuring data confidentiality. IoT Cloud users tend to adopt lightweight scheme to protect their data and delegate complex functions to the CSP for implementation. So, the users need an appropriate access control mechanism to manage the access control authority by himself, rather than giving this right to the CSP. Moreover, considering the possible data consumers in the future, we should formulate access control policies for data, not for unknown access request. In order to realize the requirements above, we've studied the relevant technologies and the achievements in recent years. In this paper, we propose a certificateless and dynamic proxy re-encryption-based data sharing scheme for IoT Cloud. In terms of the function of the scheme, we pay more attention to the protection of the original data, and on this basis, the data produced by the IoT terminal devices can be handed over to the Cloud service providers in an authorized way. In addition, our scheme ensures the confidentiality of data and can satisfy the IoT Cloud users who have low requirements for real-time but need for security data sharing. This scheme combines the certificateless public key cryptography with proxy re-encryption, while adding ciphertext evolution and conditional key mechanism to achieve the following features:

(1) Data confidentiality: user data is encrypted and then uploaded to the Cloud. Without authorization, the Cloud server and any third party cannot obtain the data;

(2) Data access control: the access control mechanism based on proxy re-encryption rather than file management system ensures more reliable access control and further reduces the security risk of semi-trusted CSP. The lightweight feature of our proposed scheme is more suitable for IoT terminal devices with poor computing performance, enabling them to achieve reliable access

*Corresponding Author: Yuanni Liu; E-mail: liuyn@cqupt.edu.cn
DOI: https://doi.org/10.70003/160792642025032602002

control with less computing overhead;

(3) Dynamics of user key: the long-term use of the same key is unsecure. In our scheme, the user can immediately update the identity and key pair once the key is leaked, or performs the update regularly, which enhances the security and privacy;

(4) Evolution of ciphertext: After updating the identity and key pair, users do not need to re-upload the encrypted data, instead commanding the CSP to perform the update calculation, making long-term data backup and maintenance feasible.

2 Related Work

Blaze et al. first proposed the concept of proxy re-encryption in 1998, and constructed a bidirectional proxy re-encryption (PRE) scheme based on ElGamal [2]. However, this scheme has security problems and cannot resist the collusion attack of delegator and delegatee, resulting in the disclosure of delegator's private key. Ateniese et al. formally defined the PRE scheme and proposed a one-way single-hop PRE algorithm based on bilinear pairings (irreversible delegation relationship, single re-encryption processing), and applied it in distributed systems [3]. Identity-based broadcast proxy re-encryption (IB-BPRE) schemes have been proposed to ensure the secure data sharing in cloud applications. Therefore, Ge et al. proposed a revocable identity-based broadcast proxy re-encryption system which address the inconvenience for cloud users [4].

The certificateless public key cryptography (CL-PKC) proposed by Al-Riyami and Paterson solves the key escrow problem in identity-based cryptosystem (IBC) [5]. In Sur et al.'s scheme, the CL-PKC is combined with PRE, so that this scheme has the advantages of both and eliminates the shortcomings of IBC scheme [6]. Based on Sur et al.'s scheme, the scheme proposed by Xu et al. is one-off and unidirectional, which can be applied to data sharing in the Cloud environment [7]. In recent years, Zhang et al.'s scheme uses a certificateless signature scheme to ensure the authenticity of data in the industrial IoT data crowdsensing system [8]. The large amount of data in the Industrial IoT makes searchability an important factor affecting efficiency. The scheme proposed by Ma et al. realizes the protection of user data and efficient data retrieval through keyword search [9]. The solution proposed by Ge et al. not only supports attribute-based keyword search but also enables attribute-based data sharing at the same time, which is in contrast to the existing solutions that only support either one of two features [10].

The functionality and security of PRE have been intensively investigated in recent years. Su et al. proposed a trusted authorization scheme based on PRE, which allows user to manage the authorization, data collection and sharing of dynamic nodes at all levels in the IoT Cloud [11]. Gao et al. described a blockchain-based scheme to authorize and revoke digital rights [12]. By using the ciphertext-policy attribute-based encryption (CPABE) and PRE, rights owner can effectively trade digital right with various right requesters. This scheme is also an application combining CPABE and PRE. To manage outsourced encrypted data sharing in clouds, Ge et al. proposed an attribute-based proxy re-encryption scheme. When the cloud service and the user are incompletely trusted, the scheme is introduced to support verifiability and fairness. [13]. In Zhan et al.'s scheme, users' private information related to healthcare is divided into different parts by content and stored separately in the cloud [14]. Matching private data only when legitimate access occurs prevents cloud servers from revealing user information. In addition to CPABE, access control is implemented using conditions for ciphertext.

In the scheme proposed by Liu et al., PRE is used to grant the first level of access to multiple users at the same time, and different numbers of conditions are used to control the exact access of a single user to the ciphertext [15]. This scheme is more suitable for the case where the structure of access users has structural characteristic. A novel security notion named revocable identity-based broadcast proxy re-encryption is presented by Ge et al. to address the issue of key revocation in this work [16]. Blockchain, meanwhile, further improve the fairness of transactions. Based on the security hardware Secure Enclave, Zhang et al. proposed a unidirectional multi-hop PRE scheme with constant ciphertext size without extension, named hPRESS [17]. With the evolution of Secure Enclave in the future, the hPRESS scheme is also scalable.

Almolhis et al. pointed out that the data security issues of IoT Cloud mainly introduced as the consequence of when data are transferred, stored and processed at Cloud which is a third-party [18]. One of the security issues is data breaches, when data is accessed by unauthorized individuals. Zhou et al. discussed the security issues associated with IoT Cloud platforms for the smart home application [19]. Based on PRE, Su et al. proposed a trusted authorization scheme for nodes on IoT Cloud [11]. Each node's status is under the authorization server's control, which could ensure the security of data.

3 System Definitions

3.1 System Model

The IoT cloud architecture provides massive storage resources and large-scale parallel computing for IoT applications. As a producer and owner of data, resource-limited IoT terminals upload data to resource-abundant Cloud server. Data delivery and service interaction are provided by Cloud. As Figure 1. shows, the following entities are included in the CL-C-PRE system model:

Key Generation Center (KGC): KGC is a fully trusted third party, responsible for the registration of all new users joining the system, the partial key generation and the identity update of existing users. The user interacts with KGC through the public channel to request its valid identity and key pair (PK, SK).

Data Owner (DO): As the delegator in the CL-C-PRE system, the data owner encrypts all his sensitive data and

upload it to the Cloud storage server to achieve secure data backup and Cloud data access control. In the application of IoT Cloud, take vehicle as an example, DO is the vehicle user, who generally has limited storage and computing capacity. Sensitive data includes driving information, other intelligent device information, user identity information, etc.

Data Consumer (DU): DU is the delegatee in the CL-C-PRE system. Data users, such as third-party value-added agencies, can send requests to DO and then obtain the data they need.

CSP-storage: The storage Cloud servers can provide storage backup and ciphertext update services for users, and sends ciphertext to CSP-proxy when DO need to authorize the DU and re-encrypt the ciphertext.

CSP-proxy: The proxy Cloud servers can re-encrypt and send the ciphertext to DU. When the proxy re-encrypts the data with the correct re-encryption key and condition key, that is, DU is authorized by DO, DU can decrypt the data correctly.

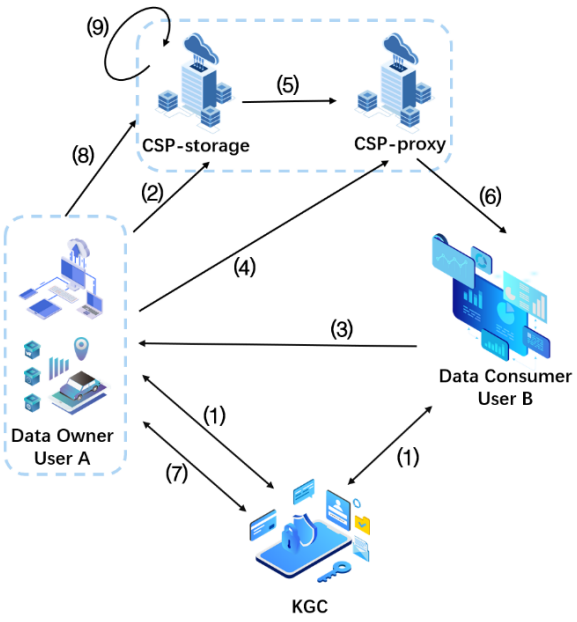


Figure 1. System model of CL-C-PRE

The complete process is described as follows:

(1) User registration and key generation: KGC run the algorithm *Setup* to initialize the system. When users join the network, they need to interact with KGC and execute the corresponding algorithms *Set_User_Partial_Key*, *Set_KGC_Partial_Key* and *Set_Full_Key* respectively to complete user registration and key generation, so as to use their valid keys to encrypt and decrypt data correctly.

(2) Data upload: DO runs the algorithm *Encrypt* to encrypt sensitive data and sends the ciphertext to CSP-storage.

(3) Data request: DU sends a request to DO to access private data.

(4) Re-encrypt authorization: When DO allows DU access to the data, DO runs the algorithm *Set_ReKey* to generate the re-encryption key and *Set_CKey* to generate the conditional key, which are sent to CSP-proxy.

(5) Cloud ciphertext transmission: CSP-storage sends the requested ciphertext to CSP-proxy.

(6) Re-encryption: After receiving the ciphertext and corresponding keys, CSP-proxy runs the algorithm *Re_Encrypt* for calculation and sends the re-encrypted ciphertext to DU. At this point, DU can decrypt with its own private key to obtain the desired data.

(7) User identity update: In case of key leakage or periodic key update, users can update their identity and key pair to KGC through the same operations as in (1).

(8) Update key generation: After updating identity, the user runs the algorithm *Key_Update* to generate the update Key for the uploaded ciphertext and send it to the CSP-storage.

(9) Ciphertext evolution: After receiving the updated key from the user, the CSP-storage runs *Update_Enc* to calculate and update the original ciphertext.

The scheme can provide secure backup and access control of Cloud privacy data by using certificateless public key cryptography, proxy re-encryption, conditional key, ciphertext evolution and other methods. CL-PKC avoids the extra cost of certificate and the key escrow problem of IBE scheme. PRE takes into account the security and access control of private data stored in the Cloud. Conditional key is mainly used to strengthen data access control and reduce security risks of semi-trusted Cloud servers. Without correct decryption conditions corresponding to the ciphertext, even if the DU has legal authorization, he cannot exceed his authority to access the data encrypted by the DO of other conditions. Ciphertext evolution enables users to update their identities and key pairs without encrypting and uploading the data again, ensuring key security and long-term efficient Cloud data backup.

3.2 Security Model

Definition 1. IND-CPA (Indistinguishability under Chosen-plaintext Attack).

Suppose that there is a PPT adversary $\mathcal{A}$ which can make as many queries as possible in polynomial time, and wins the following game with advantage $adv_{\mathcal{A}}^{(IND\text{-}CPA)}=1/2+\epsilon$. If ϵ is negligible, we say the scheme has IND-CPA security.

Setup. $\mathcal{A}$ chooses a challenge identity ID^* and send it to challenger $\mathcal{C}$. $\mathcal{C}$ runs the algorithm *Setup* to generate and publish the system parameters *params*, and run the algorithm *KeyGen* to generate the key pair (SK_{ID^*}, PK_{ID^*}) for the ID^*, and finally send the public key $PK_{ID^*} = (pk_{ID^*,1}, pk_{ID^*,2})$ to $\mathcal{A}$.

Challenge. The adversary $\mathcal{A}$ chooses two massages m_0, m_1 of equal length and send them to challenger $\mathcal{C}$. When received these massages, the challenger $\mathcal{C}$ chooses a massage m_b, $b \in_R \{0,1\}$, and gets the challenge ciphertext c^* by running the algorithm *Encrypt* to encrypt it with the secret key $SK_{ID^*} = (sk_{ID^*,1}, sk_{ID^*,2})$. Then the challenger $\mathcal{C}$ sends c^* to adversary $\mathcal{A}$.

Guess. The adversary $\mathcal{A}$ outputs a guess $d' \in \{0,1\}$ for the challenge ciphertext c^*. When $d = d'$, $\mathcal{A}$ wins the game.

3.3 Concrete Construction

1. *Setup*:

KGC first picks two cyclic groups G_1 and G_2 with same prime order q, and a bilinear pairing e: $G_1 \times G_1 \rightarrow G_2$, set $g_1 = e(g, g) \in G_2$ which $g \in_R G_1$ as a generator. And KGC selects four hash function as follows:

H_0: $G_1 \rightarrow Z_p^*$

H_1: $\{0,1\}^{l1} \rightarrow Z_p^*$

H_2: $\{0,1\}^{l2} \rightarrow G_1$

H_3: $G_2 \rightarrow \{0,1\}^{lm}$

where l_1 is the bit length of the user identity ID, public key PK and element of G_1, l_2 is the bit length of ID and condition ω, l_m is the bit length of the message m. Then KGC choose $s \in_R Z_p^*$ as its master key and calculates $P_{KGC} = g^s$ as its public key. Finally, KGC keep s secretly and publish the system parameters $params =< G_1, G_2, e, g, g_1, P_{KGC}, H_0, H_1, H_2, H_3 >$.

2. *KeyGen*:

Each user generates and maintains key pair by interacting with KGC as follows:

a. *Set_User_Partial_Key*: The user ID_A chooses $x_A \in_R Z_p^*$ as user-partial private key $sk_{A,2} = x_A$, and calculates the corresponding user-partial public key $pk_{A,2} = g^{xA}$. Then, the user sends $pk_{A,2}$ to KGC through public channels.

b. *Set_KGC_Partial_Key*: After received $pk_{A,2}$ from the user, KGC choose $r_A \in_R Z_p^*$ and calculates $R_A = g^{rA}$, $h_{1,A} = H_1(ID_A \,||\, pk_{A,2} \,||\, R_A)$, $u_A = r_A + s \cdot h_{1,A} + H_0(pk_{A,2}^s)$, and returns (u_A, R_A) to the user ID_A through public channel.

c. *Set_Full_Key*: Given (u_A, R_A) received from KGC, the user ID_A computes $t_A = u_A - H_0(P_{KGC}^{x_A})$, $h_{1,A} = H_1(ID_A \,||\, pk_{A,2} \,||\, R_A)$, and verifies: $g^{tA} = R_A \cdot P_{KGC}^{h1,A}$. If it is true, then the user ID_A believes that (u_A, R_A) is valid and computes $d_A = t_A \cdot x_A$; otherwise, applies (u_A, R_A) from KGC again. Finally, user's full private key is $SK_A = (sk_{A,1}, sk_{A,2}) = (d_A, x_A)$, and full public key is $PK_A = (pk_{A,1}, pk_{A,2}) = (g_1^{dA}, g^{xA})$.

3. *Set_ReKey*:

Given $SK_{A,2}$ of the delegator ID_A and PK_B of the delegate ID_B, the user ID_A computes the re-encryption key $rk_{A \rightarrow B} = pk_{B,1}^{sk_{A,2}} = (g^{xB})^{dA} = g^{dA\,xB}$.

4. *Set_CKey*:

Taking private key and re-encryption condition ω, the user ID_A computes $ck_{A,\omega} = H_2(ID_A \,||\, \omega)^{x_A}$.

5. *Encrypt*:

(*Level*-1 *encrypt*) *Level*-1 ciphertext obtained by encrypting message $m \in G_2$ under PK_A can be decrypted by the holder of SK_A and delegatee. The user ID_A chooses $k \in_R Z_p^*$, and computes $C_{A,r} = (g^k, mg_1^{dAk} \oplus H_3(e(g^{xA}, H_2(ID_A, \omega)^k)))$.

(*Level*-2 *encrypt*) *Level*-2 ciphertext obtained by encrypting message $m \in G_2$ under PK_A can be decrypted by user ID_A who is the only holder of SK_A. The user ID_A chooses $k \in_R Z_p^*$, and computes $C_{A,dA} = (g_1^{dAk}, mg_1^k)$, or $C_{A,xA} = (g_1^{xA\,k}, mg_1^k)$.

6. *Re_Encrypt*:

Received $rk_{A \rightarrow B}$ and $ck_{A,\omega}$ from delegator ID_A, the proxy correctly changes a *level*-1 ciphertext for user ID_A into a *level*-2 ciphertext. Firstly, proxy computes $e(rk_{A \rightarrow B}, \alpha) = e(a^{dA\,xB}, g^k) = g_1^{dA\,xB\,k}$, and

$\beta \oplus H_3(e(\alpha, ck_{A,\omega}))$

$= mg_1^{dA\,k} \oplus H_3(e(g^{xA}, H_2(ID_A, \omega)^k))$

$\oplus H_3(e(\alpha, ck_{A,\omega}))$

$= mg_1^{dA\,k}$

The re-encryption ciphertext is $C_{B,xB} = (g_1^{dA\,xBk}, mg_1^{dAk}) = (g_1^{xBk'}, mg_1^{k'})$, where $k' = d_A k$.

7. *Decrypt*:

(*Level*-1 *encrypt*) To decrypt the *level*-1 ciphertext $c = (\alpha, \beta)$, the user computes as follow:

$m = (\beta \oplus H_3(e(\alpha, ck_{A,\omega})))/\, e(\alpha, g)^{dA}$

$= mg_1^{dAk}/\, e(g^k, g)^{dA}$

(*Level*-2 *encrypt*) To decrypt the *level*-2 ciphertext $c = (\alpha, \beta)$ or the output of the algorithm *Re_Encrypt*, the user computes $m = \beta/\alpha^{1/dA} = mg_1^k/g_1^{dAk/dA}$. The ciphertext $c = (\alpha, \beta)$ encrypted under x_A can be decrypted in the same way.

When the key and Cloud ciphertext need to be updated periodically, the user ID_A can request new identity ID'_A and key pair $(SK_{A'}, PK_{A'})$ by interacting with KGC again. Then the user generates the ciphertext update key *upk* and sends it to the CSP-storage. The CSP-storage updates the ciphertext without recalculating or uploading data. Users can manage data by maintaining a list containing data identifiers and corresponding ciphertext tuples $[data_i, g^{ki}]$.

8. *Key_Update*:

To request the new key pair $(SK_{A'}, PK_{A'})$ of a new identity ID'_A, the user can interact with KGC again as the previous key generation process.

$SK_{A'} = (sk_{A',1}, sk_{A',2}) = (d'_A, x'_A)$,

$PK_{A'} = (pk_{A',1}, pk_{A',2}) = (g_1^{d'A}, g^{x'A})$.

Level-2 ciphertext update key is $upk_{A,dA}(g_1^{d'A/dA})$, $upk_{A,xA}(g_1^{x'A/xA})$. *Level*-1 ciphertext update key is $upk_{A,r} = (X, Y)$, where $X = H_3(e(\alpha, H_2(ID_A, \omega))^{xA} \oplus H_3(e(\alpha, H_2(ID'_A, \omega)^{xA'}))$. $Y = g_1^{d'A/dA}$ And then the user sends *upk* to the CSP.

9. *Update_Enc*:

When received the *upk* from ciphertext owners, the CSP updates the data as follows. Suppose that the ciphertext is $c = (\alpha, \beta)$, ciphertext update algorithm corresponds to encryption algorithm.

$upd_{level\text{-}1}$: $upk_{A,r} = (X, Y)$, $c' = (\alpha, (\beta \oplus X) \cdot Y)$,

$upd_{level\text{-}2}$: $c' = (\alpha \cdot upk_{A,dA}, \beta)$ or $c' = (\alpha \cdot upk_{A,xA}, \beta)$.

4 Security Analysis

4.1 Security of *Level*-1 Ciphertext

Theorem 1. Given $g \in G_1$, $a, b, c \in Z_p^*$, and $Q \in G_2$. The extended Decisional Bilinear Diffie-Hellman (eDBDH) problem is that given $(g, g^a, g^b, g^c, e(g, g)^{bc^2}, Q)$ the probability of output $Q = e(g, g)^{abc}$ or not is negligible (standard security). The discrete logarithm assumption is that given random p, $g \in_R G_1$ it is hard to find $a \in Z_p^*$ so that $p = g^a$ (master secret security). If the above assumptions hold, the scheme is correct and secure.

Lemma 1. Suppose that there is a PPT algorithm that can solve the eDBDH with negligible advantage ϵ. Then there exists an adversary $\mathcal{A}$ can breaks the *level*-1 ciphertext of CL-C-PRE with negligible advantage and CL-C-PRE is IND-CPA secure in standard model.

Proof. Assume that the adversary $\mathcal{A}$ distinguishes *level*-1 ciphertexts with non-negligible advantage. The eDBDH problem can be solved by stimulating $\mathcal{A}$ as follow:

1. Setup

Given an instance $(y, y^a, y^b, y^c, e(y, y)^{bc^2}, e(y, y)^d)$, challenger $\mathcal{C}$ can use $\mathcal{A}$ to decide $d = abc$. $\mathcal{C}$ set $g = y^c$ and $g_1 = e(g, g) = e(y, y)^{c^2}$. The key pair of KGC is $(s, P^{KGC} = g^s = (y^c)^s)$. To generate the key pair of target user, challenger chooses $sk_{B,2} = t$, sets $pk_{B,2} = g^t = (y^c)^t$, choose $r_B \in Z_p^*$ and $sk_{B,1} = b = (r_B + s \cdot h_{1,B}) \cdot t$. Target user's key pair is $(SK_B = (b, t), PK_B = (g_1^b, g^t) = (e(y, y)^{bc^2}, (y^c)^t))$.

$\mathcal{A}$ can make as many queries as possible in polynomial time T:

a. $rk_{x \to B}$, a re-encryption key, which is a delegate relationship to target user B from a user x, where x is corrupted by $\mathcal{A}$. $\mathcal{A}$ can run the related algorithms to generate key pairs (sk_x, pk_x) for corrupted users, and compute $rk_{x \to B} = (g^t)^{sk_{x,1}}$.

b. $rk_{B \to h}$, a re-encryption key, which is a delegate relationship to honest user h from B. The challenger chooses $rk_{(h,1)}, rk_{(h,2)} \in_R Z_p^*$, sets $rk_{B \to h} = (y^b)^{r(h,2)} = (g^{1/c})^{br(h,2)} = (g^{r(h,2)/c})^b$, computes $PK_h = (g_1^{r(h,1)}, y^{r(h,2)}) = (g_1^{r(h,1)}, g^{r(h,2)/c})$ and $SK_h = (r_{(h,1)}, r_{(h,2)}/c)$.

c. $rk_{h \to B}$, a re-encryption key, which is a delegate relationship to B from h. According to the above, challenger $\mathcal{C}$ set $rk_{h \to B} = (g^t)^{r(h,1)}$.

2. Challenge

$\mathcal{A}$ output two massages (m_0, m_1) sa challenge, where $m_0 \neq m_1$ of equal length. Challenger generates conditional key $ck_{B,\omega} = H_2(ID_B, \omega)^b$ for B, randomly selects $i \in_R \{0,1\}$, and computes challenge ciphertext $\mathcal{C}_i^*$:

$$\mathcal{C}_i^* = (y^a, m_i\, e(y, y)^d \oplus H_3(e(g^b, H_2(ID_B, \omega)^a)))$$
$$= (g^{a/c}, m_i\, e(g, g)^{d/c^2} \oplus H_3(e(g^b, H_2(ID_B, \omega)^{a/c})))$$

Then challenger $\mathcal{C}$ sends $\mathcal{C}_i^*$ to $\mathcal{A}$, and then waits for $\mathcal{A}$ to output the guess $i' \in \{0,1\}$.

3. Guess

If $i = i'$, that means the challenger $\mathcal{C}$ has determined that $d = abc$, otherwise $d \neq abc$.

4. Probability of breaking the challenge ciphertext

According to the proposed scheme, *level*-1 ciphertext can be decrypted by the holder of private key and delegatees. Therefore, the proof is as follow:

a. $\mathcal{C}_i^*$ is decrypted by the holder of private key:

Given $ck_{B,\omega}$, $\mathcal{A}$ can run the algorithm *level*-1 *decrypt* to decrypt the ciphertext $\mathcal{C}_i^* = (\alpha, \beta)$:

$$\alpha = g^{a/c},$$
$$\beta = m_i e(g, g)^{d/c^2} \oplus H_3(e(g^b, H_2(ID_B, \omega)^{a/c})),$$
$$m_i' = (\beta \oplus H_3(e(\alpha, ck_{B,\omega})))/\, e(\alpha, g)^b$$
$$= (m_i e(g, g)^{d/c^2} \oplus H_3(e(g^b, H_2(ID_B, \omega)^{a/c})) \oplus H_3(e(g^{a/c}, H_2(ID_B, \omega)^b)))/\, e(g^{a/c}, g)^b$$
$$= m_i\, e(g, g)^{d/c^2}/\, e(g, g)^{ab/c}$$

If $\mathcal{A}$ can decrypt $\mathcal{C}_i^*$ correctly, then the eDBDH problem is solved with $d = abc$.

b. $\mathcal{C}_i^*$ is re-encrypted by proxy:

Given $rk_{B \to h}$ and $ck_{B,\omega}$, $\mathcal{A}$ runs the algorithm *Re_Encrypt* and compute:

$$e(rk_{B \to h}, \alpha) = e((g^{r(h,2)/c})^b, g^{a/c}) = g_1^{abr(h,2)/c^2}$$
$$\beta \oplus H_3(e(\alpha, ck_{B,\omega}))$$
$$= m_i\, e(g, g)^{d/c^2} \oplus H_3(e(g^b, H_2(ID_B, \omega)^{a/c})) \oplus H_3(e(g^{a/c}, ck_{B,\omega}))$$
$$= m_i\, e(g, g)^{d/c^2}$$

When $d = abc$, re-encrypted ciphertext $\mathcal{C}_i^{*\prime} = (g_1^{abr(h,2)/c^2}, m_i\, e(g, g)^{d/c^2})$ can be seen as $\mathcal{C}_i^{*\prime} = g_1^{k_i r(h,2)/c}, m_i\, e(g, g)^{k_i})$ by setting $k_i = d/c^2 = abc/c^2$. So far, $\mathcal{C}_i^{*\prime}$ has the same structure as the ciphertext outputted by the algorithm *level*-2 *encrypt* which can be decrypted by h.

If the eDBDH problem can be solved with probability ϵ, then $\mathcal{A}$ can break CL-C-PRE scheme with $adv_{level\text{-}1}^{\mathcal{A}}$:

$$adv_{level\text{-}1}^{\mathcal{A}}$$
$$= Pr[i = i' \mid d = abc] \cdot Pr[d = abc] + Pr[i = i' \mid d \neq abc] \cdot Pr[d \neq abc] - 1/2$$
$$= (1/2 + \epsilon) \cdot 1/2 + 1/2 \cdot 1/2 - 1/2 = \epsilon/2$$

4.2 Security of *Level*-2 Ciphertext

Theorem 2. Given G_1 and G_2, $g \in G_1$, $a, b \in Z_p^*$, $Q \in G_1$. The Decisional Diffie-Hellman Inversion (DDHI) problem is that given (g, g^a, g^b, Q) the probability of output $Q = g^{a/b}$ or not is negligible (standard security). The discrete logarithm assumption is that given random p, $g \in_R G_1$ it is hard to find $a \in Z_p^*$ so that $p = g^a$ (master secret security). If the above assumptions hold, the scheme is correct and secure.

Lemma 2. Suppose that there is a polynomial time (PPT) algorithm that can solve the DDHI problem with negligible advantage ϵ. Then there exists an adversary $\mathcal{A}$ can breaks the *level*-2 ciphertext of CL-C-PRE with negligible advantage and CL-C-PRE is IND-CPA secure in standard model.

Proof. Assume that adversary $\mathcal{A}$ distinguishes *level*-2 ciphertexts with non-negligible advantage. The DDHI problem can be solved by stimulating $\mathcal{A}$ as follow:

1. Setup

Given a DDHI instance (g_1, g_1^a, g_1^b, Q), challenger can use adversary $\mathcal{A}$ to decide if $Q = g^{a/b}$. Challenger $\mathcal{C}$ runs the algorithm *Setup* to generate public parameters including $e(g, g) = g_1 \in G_2$ and $(s, P^{KGC} = g_1^s)$, and sends *params* to $\mathcal{A}$. And then challenger $\mathcal{C}$ generate the key pair of target user. *Level*-2 ciphertext can be encrypted or decrypted using any part of the private key by the same algorithm. To simplify the proof, the challenger chooses $a \in Z_p^*$, and set $sk_A = a$ as private key, $pk_A = g_1^a = g_1^a$ as public key.

2. Challenge

The adversary $\mathcal{A}$ outputs a challenge (m_0, m_1), where $m_0 \neq m_1$. The challenger $\mathcal{C}$ randomly selects $i \in_R \{0,1\}$, computes challenge ciphertext $\mathcal{C}_i^* = (g_1^b, m_i\, Q)$, sends $\mathcal{C}_i^*$ to $\mathcal{A}$, and waits for adversary $\mathcal{A}$ to output the guess $i' \in \{0,1\}$.

3. Guess

If $i = i'$, that means the challenger $\mathcal{C}$ has determined that $Q = g_1^{a/b}$, otherwise $Q \neq g_1^{a/b}$.

4. Probability of breaking the challenge ciphertext

According to the proposed scheme, *level*-2 ciphertext can be decrypted by the holder of private key. Given $\mathcal{C}_i^*$, $\mathcal{A}$ runs algorithm *level*-2 *decrypt* compute as follow:

$$\mathcal{C}_i^* = (\alpha, \beta) = (g_1^b, m_i\, Q)$$
$$m_i' = \beta/\, \alpha^{1/sk_A}) = m_i\, Q/(g_1^b)^{1/a}$$

If $\mathcal{A}$ can decrypt $\mathcal{C}_i^*$ correctly, then the stimulation is perfet, that is, $Q = g_1^{a/b}$. If the DDHI problem can be solved with probability ϵ, then $\mathcal{A}$ can break CL-C-PRE scheme with advantage $adv_{Level\text{-}2}^{\mathcal{A}}$:

$$adv_{Level\text{-}2}^{\mathcal{A}}:$$
$$= Pr[i = i' \mid Q = g_1^{a/b}] \cdot Pr[Q = g_1^{a/b}] +$$
$$= Pr[i = i' \mid Q \neq g_1^{a/b}] \cdot Pr[Q \neq g_1^{a/b}] - 1/2$$

$= (1/2 + \epsilon) \cdot 1/2 + 1/2 \cdot 1/2 - 1/2 = \epsilon/2$

4.3 Security of Evolution Ciphertext

The evolution ciphertext output by the algorithm *Update_Enc* has the same form as the old ciphertext. Therefore, the security of evolution ciphertext can be proved by referring to the foregoing.

5 Evaluation of Performance

In order to analyze the efficiency of the scheme, we use Java language in Windows system to implement the scheme based on JPBC library. The platform is built on a Windows 10 laptop equipped with AMD Ryzen 7 5800H, Radeon Graphics 3.20GHz and 16GB system memory.

The process of key generation and ciphertext upload in the scheme is affected by network status. So, we simplified the quantitative analysis of efficiency to ensure the accuracy of result. Firstly, the system establishment and maintenance part include system initialization, user key generation and update. The data calculation part includes various algorithms related to plaintext and ciphertext. This section will focus on the latter's time cost and efficiency analysis. Based on the configuration above, average values were taken for several experiments to obtain the run time results as shown in Table 1.

Table 1. Average calculation time

Symbols	Operations	Run time (ms)
T_e	Bilinear pairing	3.67
T_p	Modular exponentiation	5.74
T_m	Point operation in G_T	0.02
T_i	Modular inversion	0.02
T_h	Map-to-point hash	0.66
T_b	Bitwise XOR	0.02
T_{mm}	Point multiplication operation of elliptic curve	5.91

The overhead of system establishment and maintenance includes computation time and interaction time between entities. Since our scheme is implemented and tested on the local platform, the impact of network on scheme efficiency is not considered. The computation cost of data operation mainly depends on bilinear pair and modular exponentiation operation, and the rest run time can be neglected after reasonable simplification. The basic scheme CL-PRE [7] and IBP2 scheme [20] have better computational efficiency in encryption and decryption algorithm than other schemes. However, both of them have ciphertext extension and do not support conditional PRE and ciphertext evolution. In spite of adoption of elliptic curve, RIBE-CE scheme [21] has no obvious disadvantage in terms of time consumption.

Table 2. Analysis of performance in each scheme

	Proposed scheme	Basic CL-PRE [7]	IBP2 [20]	RIBE-CE [21]	IBPRE+ [24]	SS-PRE [25]	IB-PRE-FCAC [22]	CP-ABPRE-DR [26]
$Enc_{level\text{-}1}$	$3T_p + T_e$	$2T_p + T_e$	$3T_p + T_e$	$2T_p + 2T_e + T_{mm}$	$6T_p$	$8T_p$	$2T_p + T_e + nT_E$	$6T_p$
$Enc_{level\text{-}2}$	$2T_p$	$2T_p + T_e$						
RK	T_p	$3T_p + T_e$	T_e	×	$2T_p$	$2T_p$	$3T_p + 2T_e$	$10T_p$
CK	T_p	×	×	×	×	×	×	×
RE	$2T_e$	$2T_p + 2T_e$	$2T_p + 4T_e$	×	$2T_e$	$3T_p + 5T_e$	$T_p + T_e$	$T_p + T_e$
$Dec_{level\text{-}1}$	$T_p + 2T_e$	$2T_e$	$T_p + 2T_e$	$2T_e + T_{mm}$	$5T_e$	$3T_p + 3T_e$	$T_e + nT_D$	$T_p + 3\ T_e$
$Dec_{level\text{-}2}$	T_p	T_e	$4T_p + 2T_e$		$3T_e$	$2T_p + 2T_e$		$2T_p + 3\ T_e$
updRe	negligible	×	×	$2T_e$	×	×	×	×
PRE	√	√	√	×	√	√	√	√
Condition	√	×	×	×	×	×	×	×

Besides, the scheme IBPRE+ is also a message-level based fine-grained proxy re-encryption combined with identity encryption [24]. Because the implementation of this scheme depends on 3-linear map, the instability of 3-linear map hampers the practical application of the scheme. In the scheme SS-PRE [21], conditional PRE is provided by computing bilinear pairings, which results in an increase in ciphertext length. In addition, it does not support ciphertext evolution.

The scheme proposed by Lin et al. provides a different idea, which uses a symmetric encryption to encrypt and decrypt the data, transmitting the symmetric encryption ciphertext and the corresponding symmetric key in a proxy re-encryption [22]. This scheme is similar to this scheme in terms of computational overhead of encryption, re-encryption and decryption algorithms, but it also has the disadvantage of ciphertext expansion, so the scheme is single-hop, which limits the extension of application scenarios. T_E is the encryption time of symmetric encryption/decryption function which used in IB-PRE-FCAC, T_D is the decryption time. Ren et al. proposed the autonomous path proxy re-encryption, where the delegator can control the whole delegation path in a multi-hop delegation process and have a more detailed management of the proxy delegation [23]. To achieve such characteristics, the key and ciphertext in the scheme become more complex, not only the length, but also their computational overhead increases. Compared with the above two schemes, proposed scheme has higher computational efficiency and more diverse features,

which are more suitable for the IoT cloud. The scheme CP-ABPRE-DR proposed by Ge et al. is an attribute-based proxy re-encryption with direct revocation scheme [26]. The performance shown in Table 2 is derived only from the scenario when the access policy is simplest. In practical application scenarios, the computational overhead of the scheme increases linearly with the size of the access policy and attribute set. This solution is not suitable for low performance IoT Cloud terminal devices, and only performs well in scenarios where users have richer computing resources.

Combined with the result in Table 1, we compared the efficiency and performance of each scheme. The negligible run times are not considered for simplification, such as modular inversion and map-to-point hash operation. The simplified is shown in Table 2. T_s is the signature time of signature scheme which used in RIB-CPRE-CE, T_v is the verification time.

The analysis of performance in each scheme in Table 2 shows that the average time consumption of proposed encryption algorithm is lower than the basic CL-PRE, and also lower than other schemes in recent years. Moreover, the algorithms including re-encryption key generation and decryption algorithm, which bear the computational overhead by the users, are less time cost in this scheme. Below the time consumption analysis of each algorithm, the performance of each scheme is also compared in Table 2, which shows that this scheme has more performance while consuming less time.

According to the time cost statistics of Schnorr Protocol given in Bellare et al.' scheme, we get the result in Figure 2 [27]. By substituting the values in Table 1 into the items in Table 2 for calculation, the time cost from encryption, decryption and re-encryption in each scheme can be visually compared in Figure 2 in the form of a bar chart.

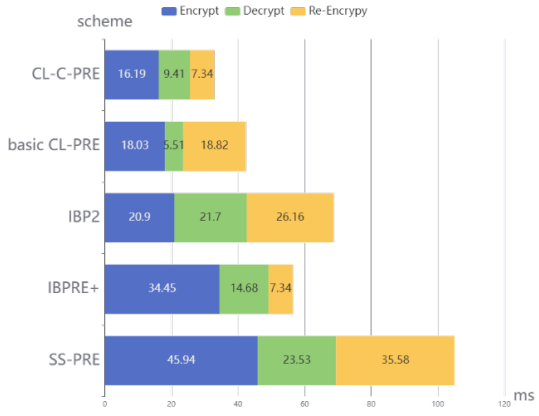


Figure 2. Cost comparisons of each scheme

Since RIBE-CE is not a PRE scheme and only considers ciphertext evolution performance, it is not included in the analysis. As can be seen from the figure, the proposed scheme CL-C-PRE not only provides various features that meet the requirements of IoT Cloud application, but also ensures the efficiency of the system without sacrificing computing costs.

6 Conclusion

To achieve reliable data sharing for IoT Cloud, we proposed a proxy re-encryption based data sharing scheme, which supports confidential storage and access control in Cloud. The key generation process is constructed based on certificateless public key cryptography, which reduces the potential security risk caused by KGC. In addition, the key update and ciphertext evolution not only meet the requirements of long-term data backup on Cloud and regular key update, but also ensure the efficiency of the system. According to the analysis, our scheme has advantages in terms of computing cost and ciphertext size.

Our scheme can provide secure backup and identity based access control, however, fine-grained access control is a practical method in real situation which need further study. In our future work, new secure data sharing with fine-grained access control based on CPABE will be investigated.

Acknowledgement

Our work was jointly supported by the National Key Research and Development Program of China (2023YFF0905300).

References

[1] L. Hou, S.-H. Zhao, X. Xiong, K. Zheng, P. Chatzimisios, M. S. Hossain, W. Xiang, Internet of things cloud: architecture and implementation, *IEEE Communications Magazine*, Vol. 54, No. 12, pp. 32-39, December, 2016.

[2] M. Blaze, G. Bleumer, M. Strauss, Divertible protocols and atomic proxy cryptography, in: K. Nyberg (Eds.), *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, Berlin, Heidelberg, 1998, pp. 127-144.

[3] G. Ateniese, K. Fu, M. Green, S. Hohenberger, Improved proxy re-encryption schemes with applications to secure distributed storage, *ACM Transactions on Information and System Security (TISSEC)*, Vol. 9, No. 1, pp. 1-30, February, 2006.

[4] C. Ge, Z. Liu, J. Xia, L. Fang, Revocable identity-based broadcast proxy re-encryption for data sharing in clouds, *IEEE Transactions on Dependable and Secure Computing*, Vol. 18, No. 3, pp. 1214-1226, May-June, 2021.

[5] S. S. Al-Riyami, K. G. Paterson, Certificateless public key cryptography, in: C. S. Laih (Eds.), *International conference on the theory and application of cryptology and information security*, Springer, Berlin, Heidelberg, 2003, pp. 452-473.

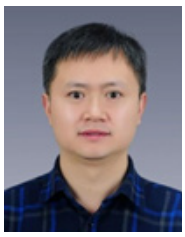
[6] C. Sur, C. D. Jung, Y. Park, K. H. Rhee, Chosen-ciphertext secure certificateless proxy re-encryption, In: B. De Decker, I. Schaumüller-Bichl (Eds.), *IFIP International Conference on Communications and Multimedia Security*, Springer, Berlin, Heidelberg, 2010, pp. 214-232.

[7] L. Xu, X. Wu, X. Zhang, CL-PRE: a certificateless proxy re-encryption scheme for secure data sharing with public cloud, *Proceedings of the 7th ACM symposium on information, computer and communications security*, Seoul, Korea, 2012, pp. 87-88.

[8] Y. Zhang, R.-H. Deng, D. Zheng, J. Li, P. Wu, J. Cao,

Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT, *IEEE Transactions on Industrial Informatics*, Vol. 15, No. 9, pp. 5099-5108, September, 2019.
[9] M. Ma, D. He, N. Kumar, K. K. R. Choo, J. Chen, Certificateless searchable public key encryption scheme for industrial internet of things, *IEEE Transactions on Industrial Informatics*, Vol. 14, No. 2, pp. 759-767, February, 2018.
[10] C. Ge, W. Susilo, Z. Liu, J. Xia, P. Szalachowski, L. Fang, Secure keyword search and data sharing mechanism for cloud computing, *IEEE Transactions on Dependable and Secure Computing*, Vol. 18, No. 6, pp. 2787-2800, November-December, 2021.
[11] M. Su, B. Zhou, A. Fu, Y. Yu, G. Zhang, PRTA: A Proxy Re-encryption based Trusted Authorization scheme for nodes on CloudIoT, *Information Sciences*, Vol. 527, pp. 533-547, July, 2020.
[12] J. Gao, H. Yu, X. Zhu, X. Li, Blockchain-Based Digital Rights Management Scheme via Multiauthority Ciphertext-Policy Attribute-Based Encryption and Proxy Re-Encryption, *IEEE Systems Journal*, Vol. 15, No. 4, pp. 5233-5244, December, 2021.
[13] C. Ge, W. Susilo, J. Baek, Z. Liu, J. Xia, L. Fang, A verifiable and fair attribute-based proxy re-encryption scheme for data sharing in clouds, *IEEE Transactions on Dependable and Secure Computing*, Vol. 19, No. 5, pp. 2907-2919, September-October, 2022.
[14] W. Zhan, Y. Chen, W. Ren, X. Ren, Y. Liu, Improved Attribute Proxy Re-encryption Scheme, in: J. Xiong, S. Wu, C. Peng, Y. Tian (Eds.), *International Conference on Mobile Multimedia Communications*, Springer, Cham, 2021, pp. 343-353.
[15] Y. Liu, Y. Ren, C. Ge, J. Xia, Q. Wang, A CCA-secure multi-conditional proxy broadcast re-encryption scheme for cloud storage system, *Journal of Information Security and Applications*, Vol. 47, pp. 125-131, August, 2019.
[16] C. Ge, W. Susilo, J. Baek, Z. Liu, J. Xia, L. Fang, Revocable attribute-based encryption with data integrity in clouds, *IEEE Transactions on Dependable and Secure Computing*, Vol. 19, No. 5, pp. 2864-2872, September-October, 2022.
[17] F. Zhang, Z.-Y. Liang, C. Zuo, J. Shao, J.-T. Ning, J. Sun, J. K. Sun, Y.-B. Bao, hpress: A hardware-enhanced proxy re-encryption scheme using secure enclave, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 40, No. 6, pp. 1144-1157, June, 2021.
[18] N. Almolhis, A. M. Alashjaee, S. Duraibi, F. Alqahtani, A. N. Moussa, The security issues in IoT-cloud: a review, *2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA)*, Langkawi, Malaysia, 2020, pp. 191-196.
[19] W. Zhou, Y. Jia, Y. Yao, L.-P. Zhu, L. Guan, Y.-H. Mao, P. Liu, Y.-Q. Zhang, Discovering and Understanding the Security Hazards in the Interactions between {IoT} Devices, Mobile Apps, and Clouds on Smart Home Platforms, *28th USENIX Security Symposium (USENIX Security 19)*, Santa Clara, CA, USA, 2019, pp. 1133-1150.
[20] M. Green, G. Ateniese, Identity-based proxy re-encryption, in: J. Katz, M. Yung (Eds.), *International Conference on Applied Cryptography and Network Security*, Springer, Berlin, Heidelberg, 2007, pp. 288-306.
[21] Y. Sun, Y. Mu, W. Susilo, F. Zhang, A. Fu, Revocable identity-based encryption with server-aided ciphertext evolution, *Theoretical Computer Science*, Vol. 815, pp. 11-24, May, 2020.
[22] H.-Y. Lin, T.-T. Tsai, P.-Y. Ting, Y.-R. Fan, Identity-Based Proxy Re-Encryption Scheme Using Fog Computing and Anonymous Key Generation, *Sensors*, Vol. 23, No. 5, Article No. 2706, March, 2023.
[23] C.-D. Ren, X.-L. Dong, J.-C. Shen, Z.-H. Cao, Y. Zhou, CLAP-PRE: Certificateless Autonomous Path Proxy Re-Encryption for Data Sharing in the Cloud, *Applied Sciences*, Vol. 12, No. 9, Article No. 4353, May, 2022.
[24] X.-A. Wang, F. Xhafa, J. Ma, Z. Zheng, Controlled secure social cloud data sharing based on a novel identity based proxy re-encryption plus scheme, *Journal of Parallel and Distributed Computing*, Vol. 130, No. 153-165, August, 2019.
[25] P. Zeng, K. K. R. Choo, A new kind of conditional proxy re-encryption for secure cloud storage, IEEE Access, Vol. 6, pp. 70017-70024, November, 2018.
[26] C. Ge, W. Susilo, Z. Liu, J. Baek, X. Luo, L. Fang, Attribute-Based Proxy Re-Encryption With Direct Revocation Mechanism for Data Sharing in Clouds, *Proceedings of the ACM Turing Award Celebration Conference*, Wuhan, China, 2023, pp. 164-165.
[27] M. Bellare, S. Shoup, Two-tier signatures, strongly unforgeable signatures, and fiat-shamir without random oracles, in: T. Okamoto, X. Wang (Eds.), *International Workshop on Public Key Cryptography*, Springer, Berlin, Heidelberg, 2007, pp. 201-216.

Biographies



Yousheng Zhou received the Ph.D. degree from Beijing University of Posts and Telecommunications, China, in 2011. He is currently a Professor with the School of Cyber Security and lnformation Law, Chongqing University of Posts and Telecommunications. His research interests include public key cryptography, blockchain, and Privacy compute.

Yurong Li received the B.E. degree in Information Security from University of Science and Technology Beijing, China, in 2019, and the M.Eng. degree in Computer Science and Technology from Chongqing University of Posts and Telecommunications, China, in 2023. Her research interests include information security, proxy re-encryption, and Cloud sharing.

Yuanni Liu received the Ph.D. degree from Beijing University of Posts and Telecommunications, China, in 2011. She is currently a Professor with the School of Cyber Security and lnformation Law, Chongqing University of Posts and Telecommunications. Her research interests include Cloud computing security and Internet of vehicles security.