Mathematical Biosciences and Engineering

MBE, 19(11): 11367–11379.
DOI: 10.3934/mbe.2022529
Received: 09 April 2022
Revised: 15 July 2022
Accepted: 01 August 2022
Published: 09 August 2022

http://www.aimspress.com/journal/MBE

Research article

Secure access control using updateable attribute keys

Han-Yu Lin*, Tung-Tso Tsai, Hong-Ru Wu and Miao-Si Ku

Department of Computer Science and Engineering, National Taiwan Ocean University, Taiwan

* **Correspondence:** Email: hanyu@mail.ntou.edu.tw; Tel: +886224622192 ext 6656; Fax: +886224623249.

Abstract: In the era of cloud computing, the technique of access control is vital to protect the confidentiality and integrity of cloud data. From the perspective of servers, they should only allow authenticated clients to gain the access of data. Specifically, the server will share a communication channel with the client by generating a common session key. It is thus regarded as a symmetric key for encrypting data in the current channel. An access control mechanism using attribute-based encryptions is most flexible, since the decryption privilege can be granted to the ones who have sufficient attributes. In the paper, the authors propose a secure access control consisting of the attributed-based mutual authentication and the attribute-based encryption. The most appealing property of our system is that the attribute keys associated with each user is periodically updatable. Moreover, we will also show that our system fulfills the security of fuzzy selective-ID assuming the hardness of Decisional Modified Bilinear Diffie-Hellman (DMBDH) problem.

Keywords: access control; attribute key; authentication; encryption; updatable

1. Introduction

With the prevalence of mobile devices and the development of wide networks, all kinds of remote access applications are coming out. In a typical client-server paradigm [1,2], a remote user can request many networking services from the server which must verify the membership of the former for ensuring the data confidentiality [3] and integrity [4]. For the sake of secure communication, user authentication [5] is a commonly adopted approach. Generally speaking, user authentication can be based on passwords, biometrics and physical objects such as smart cards, tokens, keys, etc. In each authentication type, a user must register to the remote server first, which is referred to as enrollment. Then the user could login to the server for accessing various data and services.

In 1981, Lamport [6] introduced an authentication scheme in which the user has to provide his/her passwords for gaining the access privilege. Their scheme relied on a public channel, rather than a

secure one to authenticate users. In addition, the user passwords stored in the server database are in the form of hashed ones, so as to improve the confidentiality. Although the adversary can still plot the password guessing attack, the computational complexity is increased. However, their protocol was later proved to be insecure by [7].

Considering the static user identity is easily compromised during the remote login process, Das et al. [8] addressed a user authentication scheme by employing the dynamic ID. That is, a user first generates a pseudo identity before performing the login process. Even if the pseudo identity is intercepted by any eavesdropper, he/she cannot invert it to the original one. It is thus can be seen that their scheme offers better protection of user anonymity. Nevertheless, their scheme is vulnerable to some active attacks pointed by [9].

In the most existing authentication mechanisms using passwords, the remote server often keeps a so-called hashed password table for verifying users. Although these passwords are stored in the hashed form, it still has high possibility of leaking out. In particular, an adversary learning the hashed password table can launch the offline brute-force attack to break some weak passwords. To deal with this issue, in 2011, Khan et al. [10] presented a variant of remote user authentication protocols that removes the necessity of maintaining a password table. Still, any password-based authentication scheme faces a big challenge in practice, as the human beings are incapable of remembering strong passwords

For the recent years, the attribute-based cryptography [11–18] has received much attention due to its flexibility and is suitable for the fine-grained access control. In 2014, Zhu et al. [19] realized the notion of so-called fuzzy attribute-based authentication. In precise, each user owns a set of descriptive attributes which are regarded as the identity associated with the user. The private keys of the user are also related to his/her attributes. When a user has sufficient attribute (keys), he/she is able to recover the constant value of a secret polynomial and then decrypts the corresponding ciphertext. However, a later research [20] showed that their system cannot resist the notorious collusion and impersonation attacks. To solve the above security problems, Yun et al. [20] prepared different polynomials for different users such that the attribute keys of more than one user cannot be jointly integrated.

Extending from Yun et al.'s work, in 2019, Lin et al. [21] further proposed a new user authentication protocol achieving mutual authentication and supporting time-bounded keys. The property of time-bounded keys can limit the ability of users to decrypt ciphertexts after the validation period has expired. However, their scheme does not support the functionality of cloud storage using attribute-based mechanisms. In the same year, Hao et al. [22] proposed an attribute-based access control with authorized search in cloud storage. In particular, their scheme combines the technique of key delegation with key-policy attribute-based encryption to allow users to customize search policies. Xie et al. [23] designed a three-layer structure for securely accessing data in the mobile clouds using the modified hierarchical attribute-based encryption. Considering the applications of cloud-based multi-server data, Roy et al. [24] provided a fine-grained data access control mechanism. Their scheme is provably secure in the real-or-random model. However, their work does not support attribute-based mechanisms.

In 2020, Hong et al. [25] integrated time-release encryption with ciphertext-policy attribute-based encryption to access time-sensitive data in public clouds. Specifically, the data owner can grant the access right to various users according to different release time. In 2022, Ma et al. [26] introduced a server-aided fine-grained access control mechanism supporting robust revocation. With the assistance of the structure of cloud computing, their scheme could outsource the decryption overheads to the public cloud server. Consequently, the data user only performs one exponentiation computation. Nevertheless, most of previous works cannot support the functionality of key-update and hence fail to deal with the issue of key-compromise. Table 1 summarizes the limitations of current related works.

Table 1. The limitation of related works.

Scheme	Limitation
Zhu et al. [19]	Cannot support attribute-based cloud storage and key-update
Yun et al. [20]	Cannot support attribute-based cloud storage and key-update
Lin et al. [21]	Cannot support attribute-based cloud storage
Hao et al. [22]	Cannot support key-update
Xie et al. [23]	Cannot support key-update
Roy et al. [24]	Cannot support attribute-based cloud storage and key-update
Hong et al. [25]	Cannot support key-update
Ma et al. [26]	Cannot support key-update

Based on Lin et al.'s authentication protocol [21], in this paper, the authors introduce a fuzzy identity-based access control system consisting of an attribute-based mutual authentication and an attribute-based encryption. Both of the two attribute-based mechanisms support the superior characteristic of updateable attribute keys, which could provide more application flexibility in practice.

We arrange the remaining sections as follows. In the next preliminary section, we will first introduce the essential mathematical backgrounds along with the utilized cryptographic assumption. The proposed access control system will be formally described in Section 3. We analyze and prove the security of the proposed system in Section 4. At last, a conclusion remark of this work is stated in Section 5.

2. Preliminaries

We introduce the Lagrange interpolation [27,28] and the bilinear pairing [29–31] as described below:

Lagrange Interpolation

Let $f(x)$ be a polynomial of the degree $(t-1)$. Given any t points, say $(x_i, y_i = f(x_i))$ for $i \in [1, t]$ and $x_i \in Z_p^*$, we could reconstruct the polynomial $f(x)$ as:

$$f(x) = \sum_{i=1}^{t} \left[f(x_i) \prod_{j \in [1,t], j \neq i} \frac{x - x_j}{x_i - x_j} \right]$$

The Lagrange coefficient $\Delta_{i,S}$ can be expressed as

$$\Delta_{i,S} = \prod_{a \in S, a \neq i} \frac{x-a}{i-a}, \text{ for } i \in Z_p \text{ and } S \subseteq Z_p.$$

Bilinear Pairing

Let $\boldsymbol{G}_1$ and $\boldsymbol{G}_2$ separately be a multiplicative group of the same prime order p. The symbol g is a generator of $\boldsymbol{G}_1$. A bilinear pairing written as e: $\boldsymbol{G}_1 \times \boldsymbol{G}_1 \rightarrow \boldsymbol{G}_2$ satisfying the following characteristics:

(i) Bilinearity:

Given $g_a, g_b, g_c \in \boldsymbol{G}_1$[3] and two integers $i, j \in Z_p^*$, we can obtain

$$e(g_a^i, g_b^j) = e(g_a, g_b)^{ij};$$

$$e(g_a, g_b) = e(g_b, g_a);$$

$$e(g_a g_c, g_b) = e(g_a, g_b) e(g_c, g_b);$$

(ii) Non-degeneracy:

There is a generator $g \in \boldsymbol{G}_1$ fulfilling that $e(g_1, g_1) \neq 1$.

(iii) Computability:

For any element g_a and g_b of the group $\boldsymbol{G}_1$, $e(g_a, g_b)$ could be efficiently computed by a polynomial-time algorithm.

Decisional Modified Bilinear Diffie-Hellman (DMBDH) Problem

Given g^f, g^s, $g^k \in \boldsymbol{G}_1{}^3$ for some positive f, s, $k \in Z_p{}^*$, and $(e(g,g)^{\frac{fs}{k}}, \delta) \in \boldsymbol{G}_2{}^2$, the decisional modified bilinear Diffie-Hellman (DMBDH) problem is to determine if $e(g,g)^{\frac{fs}{k}}$ equals to δ or not.

Decisional Modified Bilinear Diffie-Hellman (DMBDH) Assumption

The DMBDH assumption states that for any polynomial-time adversary, the advantage to solve the DMBDH problem is negligible.

3. The proposed scheme

On the basis of the work [21], we introduce a fuzzy identity-based access control mechanism with dynamically updateable keys in this section.

3.1. Algorithms

The proposed access control system consists of six algorithms including Setup, KeyExtract, Authentication, Encryption, Decryption and Key-update. We describe each algorithm as follows:

Setup: Taking as input a security parameter, the cloud server first chooses necessary system parameters including the public values, master secret keys (*msk*) along with a time key.

KeyExtract: Each user can request his/her attribute keys from the cloud server.

Authentication: It is an interactive process between the user and the cloud server. That is, a user can login to the cloud server if the authentication result is successful.

Encryption: An authenticated user can encrypt the data and then upload the ciphertext to the cloud server.

Decryption: A user can request the ciphertext from the cloud server and then decrypt it with his/her attribute keys.

Key-update: Any legitimate user is able to renew his/her private keys for the coming time periods by the assistance of the cloud server.

3.2. Construction

The authors present a concrete construction according to the above algorithms. Details of each algorithm are shown as follows:

Setup: Given a security parameter l, the cloud server first determines two multiplicative groups $\boldsymbol{G}_1$ and $\boldsymbol{G}_2$ with the same prime order p. Let g be a generator of the group $\boldsymbol{G}_1$ and e: $\boldsymbol{G}_1 \times \boldsymbol{G}_1 \rightarrow \boldsymbol{G}_2$ a bilinear map. There is also a secure hash function H which accepts a variable-length input and returns a fixed-length output. Let $\boldsymbol{W} = \{w_1, w_2, \ldots, w_n\}$ be the universe of all attributes. Then the cloud server executes the following initialization steps:

1) Randomly select $k_1, k_2, \ldots, k_n \in_R Z_p{}^*$ to compute

$$\{K_i = g^{k_i}\}_{i\in[1,\ n]}; \tag{1}$$

2) Determine $a_1, a_2, \ldots, a_n \in \{0, 1\}$. Specifically, when w_i is authorized by the cloud server, $a_i = 1$; else, $a_i = 0$. Define the set $A = \{a_i\}_{i\in[1,\ n]}$ and compute

$$I = \sum_{i=1, a_i\neq 0}^{n} (g^{w_i} a_i); \tag{2}$$

3) Randomly select $z \in Z_p^*$ to compute

$$Z = e(g,\ g)^z; \tag{3}$$

4) Announce the public key $PK = (\{K_i\}_{i\in[1,\ n]}, Z, A\}$;
5) Define the master secret key $msk = (\{k_i\}_{i\in[1,\ n]}, z\}$;
6) Randomly select $v \in_R Z_p^*$ and define it as the time key mtk.

KeyExtract: A user id_u owning the attribute set $\boldsymbol{W_u} \subseteq \boldsymbol{W}$ such that $|\ \boldsymbol{W_u}\ | = t$ is able to request his/her attribute keys from the cloud server. The cloud server first determines a $t - 1$ polynomial $f_{id_u}(x)$ in which the constant is z and then derives the attribute keys as

$$\{S_i = g^{\frac{f_{id_u}(i)}{k_i(id_u+v)}}\}_{i\in W_u} \tag{4}$$

The user id_u will receive the attribute keys $\{S_i\}_{i\in \boldsymbol{W}_u}$ via secure communication.

Authentication: To login the cloud server, a user id_u executes the following processes with the cloud server interactively:

i. The user first delivers (id_u, $\boldsymbol{W_u}$) to the cloud server.
ii. When receiving it, the cloud server randomly selects $R \in \boldsymbol{G}_2$ and $r \in Z_p^*$ to compute

$$Q_0 = RZ^r \tag{5}$$

$$\{Q_i = K_i^{r(id_u\ +\ v)}\}_{i\in \boldsymbol{W}_u} \tag{6}$$

Then (Q_0, $\{Q_i\}_{i\in \boldsymbol{W}_u}$) are sent back to id_u.

iii. When receiving it, id_u computes

$$R' = \frac{Q_0}{\prod_{i\in W_u} e(S_i,\ Q_i)^{\Delta_{i,W_u}(0)}} \tag{7}$$

$$C_1{}' = \prod_{w_i\in W_u} g^{w_i} \tag{8}$$

$$C_2' = H(R' \ ||\ C_1' \ ||\ TS) \tag{9}$$

where TS is a timestamp. The message (C_2', TS) is transmitted the cloud server.

iv. The cloud server verifies whether $|\ TS' - TS\ | \leq \Delta T$ where TS' is the current time and ΔT is a predefined time interval. If it holds, the cloud server proceeds to the next step; else, it rejects the login request.
v. Compute

$$C_2 = H(R \ ||\ C_1 \ ||\ TS). \tag{10}$$

If $C_2' = C_2$, the cloud server continues to derive

$$C_3 = H(id_u \ ||\ R \ ||\ C_1 \ ||\ TS') \tag{11}$$

and sends (C_3, TS') to id_u.

vi. If $|TS'' - TS'| \leq \Delta T$, id_u derives

$$C_3' = H(id_u \,||\, R' \,||\, C_1' \,||\, TS'); \tag{12}$$

and checks if $C_3' = C_3$. When the equality holds, the interactive authentication process is viewed as successful. We illustrate the above processes in Figure 1.

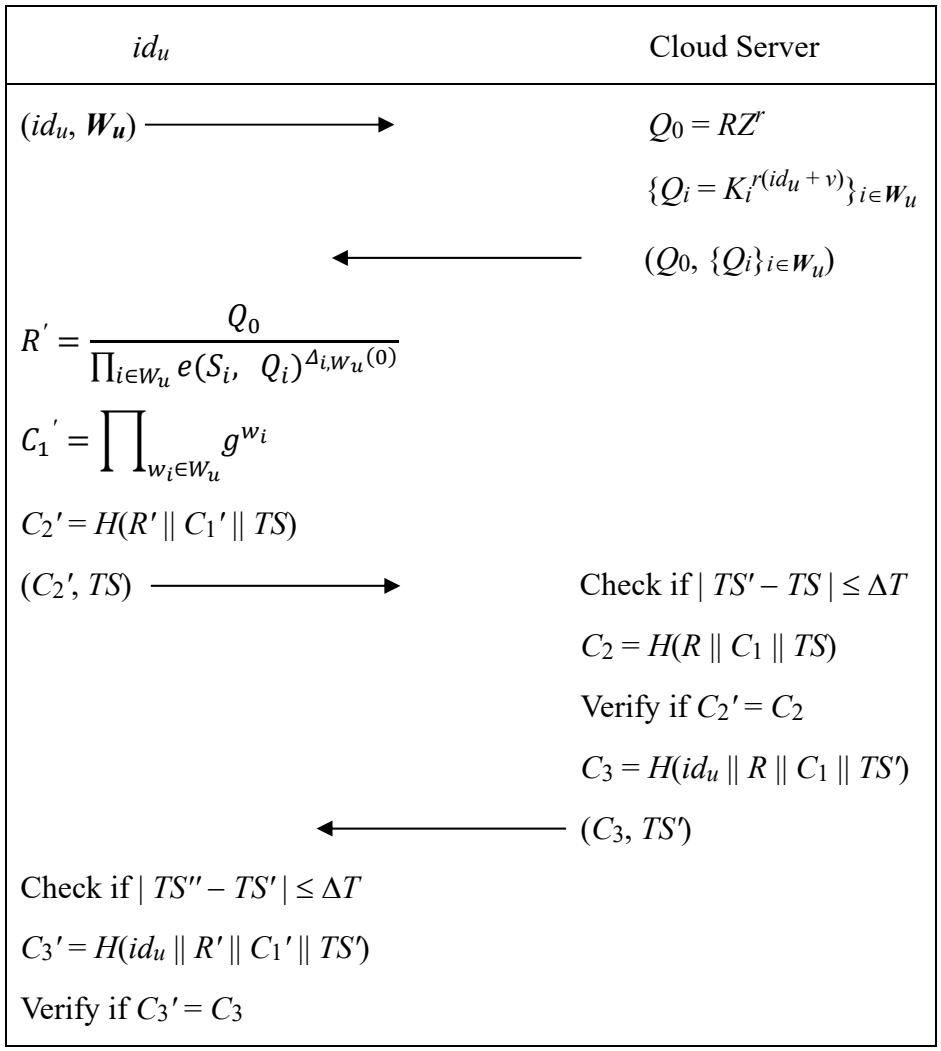

Figure 1. Illustration of authentication processes.

Encryption: To encrypt a message M for storing in the cloud server, an authenticated user id_u executes the following processes:

a) Randomly select $d \in Z_p^*$ to compute

$$CT = M \cdot (Q_0/R')^d \tag{13}$$

$$CT_i = \{Q_i^d\}_{i \in \boldsymbol{W}_u} \tag{14}$$

b) Upload the ciphertext $(id_u, CT_{index}, CT, \{CT_i\}_{i \in \boldsymbol{W}_u})$ to the cloud server. Here, CT_{index} is the category name of the ciphertext.

Decryption: To decrypt a ciphertext $(CT, \{CT_i\}_{i \in \boldsymbol{W}_u})$ which is downloaded from the cloud server, id_u utilizes his/her attribute keys to compute

$$M = \frac{CT}{\prod_{i \in W_u} e(S_i, CT_i)^{\Delta_{i,W_u}(0)}} \tag{15}$$

Key-update: To periodically update the attribute keys, the cloud server first chooses $v' \in_R Z_p^*$ as the new *mtk*, and then computes

$$h = (id_u + v)(id_u + v')^{-1} \tag{16}$$

The parameter h is delivered to id_u. Consequently, id_u is able to renew his/her attribute keys as

$$\{S_i' = S_i^h\}_{i \in W_u}. \tag{17}$$

4. Algorithm and security analyses

In this section, we first show that the proposed access control mechanism is correct and then formally prove the fuzzy selective-ID security of our protocol.

4.1. Correctness

We demonstrate that a valid user can successfully login to the cloud server and decrypt the corresponding ciphertext with his/her attribute keys.

Theorem 1. *A valid user id_u can be authenticated by the cloud server if $R' = R$.*

Proof: Derived from Eq (7), we have

$$\begin{aligned} R' &= \frac{Q_0}{\prod_{i \in W_u} e(S_i,\ Q_i)^{\Delta_{i,W_u}(0)}} \\ &= \frac{RZ^r}{\prod_{i \in W_u} e(g^{\frac{f_{id_u}(i)}{k_i(id_u+v)}},\ K_i{}^{r(id_u+v)})^{\Delta_{i,W_u}(0)}} && \text{(By Eq (5))} \\ &= \frac{R \cdot e(g,g)^{zr}}{\prod_{i \in W_u} e(g^{\frac{f_{id_u}(i)}{k_i(id_u+v)}},\ (g^{k_i})^{r(id_u+v)})^{\Delta_{i,W_u}(0)}} && \text{(By Eqs (3) and (1))} \\ &= \frac{R \cdot e(g,g)^{zr}}{e(g,g)^{zr}} && \text{(By Lagrange Interpolation)} \\ &= R \end{aligned}$$

Theorem 2. *A valid user id_u can decrypt the cloud ciphertext with Eq (15).*

Proof: Derived from the right side of Eq (15), we have

$$\begin{aligned} &\frac{CT}{\prod_{i \in W_u} e(S_i, CT_i)^{\Delta_{i,W_u}(0)}} \\ &= \frac{M(Q_0/R')^d}{\prod_{i \in W_u} e(g^{\frac{f_{id_u}(i)}{k_i(id_u+v)}},\ K_i{}^{rd(id_u+v)})^{\Delta_{i,W_u}(0)}} && \text{(By Eqs (4), (6), (13) and (14))} \\ &= \frac{M \cdot e(g,g)^{zdr}}{\prod_{i \in W_u} e(g^{\frac{f_{id_u}(i)}{k_i(id_u+v)}},\ (g^{k_i})^{rd(id_u+v)})^{\Delta_{i,W_u}(0)}} && \text{(By Eqs (1), (3) and (5))} \\ &= \frac{M \cdot e(g,g)^{zdr}}{e(g,g)^{zdr}} && \text{(By Lagrange Interpolation)} \\ &= M \end{aligned}$$

4.2. Security proofs

To prove that our system achieves the fuzzy selective-ID security, we first give the corresponding definition below.

Definition 1. (Fuzzy Selective-ID) *An identity-based encryption (IBE) scheme achieves the fuzzy selective-ID security if in the following game, there is no probabilistic adversary $\mathcal{A}$ who is able to defeat a polynomial-time challenger $\mathcal{B}$ with non-negligible advantage:*

Setup: In the beginning, the adversary $\mathcal{A}$ determines the target identity id^*. Then the challenger $\mathcal{B}$ performs the Setup(1^l) algorithm to initialize public parameters and the master secret key msk. Then the public parameters are sent to $\mathcal{A}$.

Phase 1: The adversary $\mathcal{A}$ can adaptively make the queries for any id such that $| \boldsymbol{W}_{id} \cap \boldsymbol{W}_{id^*} | < t$:

KeyExtract (KE) Queries: In this query, the adversary $\mathcal{A}$ will provide an identity id for the challenger $\mathcal{B}$ who then calls the KeyExtract algorithm to get the corresponding private key S_{id} and returns it.

Authentication (AU) Queries: In this query, the adversary $\mathcal{A}$ will provide an identity id for the challenger $\mathcal{B}$ who then calls the authentication algorithm and returns an authentication token (Q_0, $\{Q_i\}_{i \in \boldsymbol{W}_{id}}$).

Challenge: The adversary $\mathcal{A}$ determines two messages (M_0, M_1) of the same length. Next, the challenger $\mathcal{B}$ takes the input of (id^*, M_λ) where $\lambda \in_R \{0, 1\}$ to produce a ciphertext (id^*, CT^*_{index}, CT^*, $\{CT_i^*\}_{i \in \boldsymbol{W}_{id^*}}$) as the challenge for $\mathcal{A}$.

Phase 2: Upon receiving the challenge, the adversary $\mathcal{A}$ is allowed to further make queries defined as those in phase 1.

Guess: When phase 2 terminates, the adversary $\mathcal{A}$ outputs a bit λ'. If $\lambda' = \lambda$, $\mathcal{A}$ is the winner of the game. Consequently, the advantage of $\mathcal{A}$ is defined as $Adv(\mathcal{A}) = | \Pr[\lambda' = \lambda] - 1/2 |$.

Theorem 3. (Proof of Fuzzy Selective-ID) *The proposed scheme achieves the fuzzy selective-ID security under the Decisional Modified Bilinear Diffie-Hellman (DMBDH) assumption. In particular, if a probabilistic polynomial-time adversary $\mathcal{A}$ breaks the fuzzy selective-ID security of our mechanism with the non-negligible advantage ε, a simulator $\mathcal{B}$ playing the DMBDH game with the non-negligible advantage $(1/2)\varepsilon$ can be constructed.*

Proof: Let $(g, g^f, g^s, g^k, e(g,g)^{\frac{fs}{k}}, \delta)$ be a problem instance of DMBDH for $\mathcal{B}$ whose purpose is to decide if $e(g, g)^{fsk}$ equals to δ or not by utilizing the advantage of $\mathcal{A}$.

Setup: In the beginning, the adversary $\mathcal{A}$ determines the target identity id^* and the challenger performs the Setup (1^l) function to initialize public parameters $\{\boldsymbol{G}_1, \boldsymbol{G}_2, e, g, p\}$. The challenger also chooses a bit b which $\mathcal{B}$ does not know. If $b = 0$, the challenger sets $\delta = e(g,g)^{\frac{fs}{k}}$; else, it lets $\delta = e(g, g)^{\tau}$ for a random τ. Then $\mathcal{B}$ sets $Z = e(g^f, g)$, $A = \{a_i\}_{i \in [1, n]}$, $I = \sum_{i=1, a_i \neq 0}^{n} (g^{w_i} a_i)$ for all authorized a_i's and $mtk = v$ for $v \in_R Z_p^*$. Additionally, $\mathcal{B}$ sets $K_i = (g^k)^{r_i}$ where $r_i \in Z_p^*$ for $i \in \boldsymbol{W}_{id^*}$. If $i \in \boldsymbol{W} - \boldsymbol{W}_{id^*}$, $\mathcal{B}$ sets $K_i = g^{k_i}$ where $k_i \in Z_p^*$. Then the parameters (Z, $\{K_i\}_{i \in [1, n]}$, I) are sent to the adversary $\mathcal{A}$.

Phase 1: $\mathcal{B}$ responds to the queries made by $\mathcal{A}$ as follows:

KeyExtract (KE) Queries: For the KE query of any id such that $| \boldsymbol{W}_{id} \cap \boldsymbol{W}_{id^*} | < t$, we first let the set $\boldsymbol{W}_c = \boldsymbol{W}_{id} \cap \boldsymbol{W}_{id^*}$, $\boldsymbol{W}_d$ be any set satisfying that $\boldsymbol{W}_c \subseteq \boldsymbol{W}_d \subseteq \boldsymbol{W}_{id}$ and $| \boldsymbol{W}_d | = t - 1$, and $\boldsymbol{W}_s = \boldsymbol{W}_d \cup \{0\}$. Now we define the key component $i \in \boldsymbol{W}_d$ as follows.

1) When $i \in \boldsymbol{W}_c$, $\mathcal{B}$ sets $S_i = g^{\frac{z_i}{(id+v)}}$ where $z_i \in_R Z_p^*$.

2) When $i \in \boldsymbol{W}_d - \boldsymbol{W}_c$, $\mathcal{B}$ sets $S_i = g^{\frac{h_i}{k_i(id+v)}}$ where $h_i \in_R Z_p^*$.

Specifically, we implicitly define a $t-1$ degree polynomial $f_{ID}(x)$ with $f_{ID}(0) = f$ and $t-1$ points which are calculated as the above. That is, $f_{id}(i) = k \cdot r_i \cdot z_i$ for $i \in \boldsymbol{W}_c$ and $f_{id}(i) = h_i$ for $i \in \boldsymbol{W}_d - \boldsymbol{W}_c$. Still, when $i \notin \boldsymbol{W}_d$, $\mathcal{B}$ can also use the Lagrange interpolation for computing the private key S_i as

$$S_i = (\prod_{j \in W_c} (g^k)^{\frac{r_j z_j \triangle_{j,S}(i)}{k_i(id+v)}})(\prod_{j \in W_d - W_c} g^{\frac{h_j \triangle_{j,S}(i)}{k_i(id+v)}})(g^f)^{\frac{\triangle_{0,S}(i)}{k_i(id+v)}}$$

Consequently, it can be seen that the simulator $\mathcal{B}$ is able to respond to any PK query submitted by $\mathcal{A}$ and the returned private keys have the same distribution as those in the real scheme.

Authentication (AU) Queries: For the AU query of any id, $\mathcal{B}$ first chooses $R \in \boldsymbol{G}_2$, $r \in Z_p^*$ to compute $Q_0 = RZ^r$ and $\{Q_i = K_i^{r(id_u + v)}\}_{i \in \boldsymbol{W}_{id}}$. Then $\mathcal{B}$ returns $(Q_0, \{Q_i\}_{i \in \boldsymbol{W}_{id}})$ to $\mathcal{A}$.

Challenge: The adversary $\mathcal{A}$ determines two messages (M_0, M_1) of the same length. Next, the challenger $\mathcal{B}$ takes the input of (ID^*, M_λ) where $\lambda \in_R \{0, 1\}$ to produce a ciphertext $(id^*, CT^*_{index}, CT^*, \{CT_i^*\}_{i \in \boldsymbol{W}_{id^*}})$ in which $CT^* = M_\lambda \cdot \delta$ and $\{CT_i^* = (g^s)^{r_i(id^* + v)}\}_{i \in \boldsymbol{W}_{id^*}}$.

When $b = 0$, we know that $\delta = e(g,g)^{\frac{fs}{k}}$. That is,

$$CT^* = M_\lambda \cdot \delta = M_\lambda \cdot e(g,g)^{\frac{fs}{k}} = M_\lambda Z^{dr} \qquad \text{where } dr = \frac{s}{k}$$

$$CT_i^* = (g^s)^{r_i(id^* + v)} = g^{\frac{s}{k} k r_i (id^* + v)} = (g^{k r_i})^{\frac{s}{k}(id^* + v)} = K_i^{dr(id^* + v)} \qquad \text{where } dr = \frac{s}{k}$$

It is thus can be seen that the simulated challenge is a valid ciphertext for M_λ and the target identity id^*. Nevertheless, when $b = 1$, we have $\delta = e(g, g)^\tau$ for a random τ, meaning that the ciphertext component CT^* is a random element of $\boldsymbol{G}_2$ and the adversary $\mathcal{A}$ has no better advantage in guessing λ'.

Phase 2: When receiving the challenge, $\mathcal{A}$ is allowed to further make queries as those in phase 1.

Guess: When phase 2 terminates, the adversary $\mathcal{A}$ returns a bit λ'. If $\lambda' = \lambda$, $\mathcal{B}$ will output $b' = 0$ meaning that $\delta = e(g,g)^{\frac{fs}{k}}$. Otherwise, $\mathcal{B}$ outputs $b' = 1$ to indicate that $\delta = e(g, g)^\tau$ for a random τ.

Analysis: Let us consider two cases of the bit b. When $b = 1$, the adversary $\mathcal{A}$ has no better advantage in guessing λ'. Therefore, we have $\Pr[\lambda' \neq \lambda \mid b = 1] = 1/2$. If $\lambda' \neq \lambda$, $\mathcal{B}$ will output 1. In this case, it is obvious that $\Pr[b' = b \mid b = 1] = 1/2$. When $b = 0$, the challenge ciphertext is valid. Hence, we have $\Pr[\lambda' = \lambda \mid b = 0] = 1/2 + \varepsilon$ where ε is the advantage of the adversary $\mathcal{A}$ by our definition. If $\lambda' = \lambda$, $\mathcal{B}$ will output 0. That is, $\Pr[b' = b \mid b = 0] = 1/2 + \varepsilon$. Consequently, we can derive the advantage of $\mathcal{B}$ to solve the DMBDH problem as

$$\begin{aligned} &(1/2)\Pr[\lambda' = \lambda \mid b = 1] + (1/2)\Pr[\lambda' = \lambda \mid b = 0] - 1/2 \\ &= (1/2)(1/2) + (1/2)(1/2 + \varepsilon) - 1/2 \\ &= (1/2)\varepsilon \end{aligned}$$

4.3. Comparison

In this subsection, we evaluate the functionality and performance among the proposed and related schemes including Zhu et al.'s (ZZQ+ for short) [19], Yun et al.'s (YKL for short) [20] and Lin et al.'s

(LTW for short) [21]. The results of functionality comparisons are summarized in Table 2. It is obvious that both the ZZQ+ and YKL schemes are vulnerable to several known attacks and fail to satisfy the evaluated functionalities. Although the LTW scheme is secure against all known attacks, it cannot support the functionality of cloud storage using the mechanism of asymmetric encryption/decryption.

Table 2. Comparisons of functionalities.

	ZZQ+	YKL	LTW	Proposed
Withstand man-in-the-middle attack	Yes	Yes	Yes	Yes
Withstand replay attack	Yes	Yes	Yes	Yes
Withstand collusion attack	No	Yes	Yes	Yes
Withstand impersonation attack	No	Yes	Yes	Yes
Withstand server-spoofing attack	No	No	Yes	Yes
Support mutual authentication	No	No	Yes	Yes
Support key update	No	No	Yes	Yes
Support cloud storage	No	No	No	Yes

For better understanding of the results of performance evaluation, we first define some utilized symbols below:

n: the number of all attributes in the system;

$|W_u|$: the number of attributes of the user id_u;

B: a bilinear pairing computation;

E: an exponentiation computation;

H: a collision-resistant hash function;

We summarize the detailed performance evaluation in Table 3. From this table, one can see that the proposed scheme still maintains the same computational complexity compared with related works. Although the authentication algorithm of our scheme has to take an additional hash function, it is a worthy trade-off to achieve the characteristic of mutual authentication.

Table 3. Performance evaluation.

	ZZQ+	YKL	LTW	Proposed
Setup	$(2n)E + B$	$(2n)E + B$	$(2n)E + B$	$(2n)E + B$
KeyExtract	$\|W_u\|E$	$\|W_u\|E$	$\|W_u\|E$	$\|W_u\|E$
Authentication (server)	$(\|W_u\| + 1)E + H$	$(\|W_u\| + 1)E + H$	$(\|W_u\| + 1)E + H$	$(\|W_u\| + 1)E + H$
Authentication (user)	$(\|W_u\|)(2E + B) + H$	$(\|W_u\|)(2E + B) + H$	$(\|W_u\|)(2E + B) + 2H$	$(\|W_u\|)(2E + B) + 2H$
Encryption	N.A.	N.A.	N.A.	$(\|W_u\| + 1)E$
Decryption	N.A.	N.A.	N.A.	$(\|W_u\|)(E + B)$
Key-update	N.A.	N.A.	$\|W_u\|E$	$\|W_u\|E$

**Note*: the symbol of "N.A." stands for not available

5. Conclusions

Elaborating on the merits of attribute-based cryptography, in this paper, the authors come up with a provably secure fuzzy identity-based access control system supporting updateable attribute keys. In particular, the proposed system consists of both the fuzzy identity-based mutual authentication and the fuzzy identity-based encryption. That is, the former mechanism allows a user to login the remote server

via his/her attribute keys while the latter further enables the authenticated user to decrypt the server ciphertext if his/her attribute keys satisfy the ciphertext access policy. Our access control system permits the users to update their attribute keys periodically, so as to solve the key-compromise problem. When compared with most existing attribute-based schemes which do not support key update, our system is more appealing the practical environments. Additionally, we also demonstrate that our scheme is provably secure in the notion of fuzzy selective-ID security under the DMBDH assumption.

Acknowledgements

This work was supported in part by the Ministry of Science and Technology of Republic of China under the contract numbers MOST 110-2221-E-019-041-MY3 and MOST 110-2222-E-019-001-MY2.

Conflict of interest

The authors declare there is no conflict of interest.

References

1. M. Lim, C2CFTP: direct and indirect file transfer protocols between clients in client-server architecture, *IEEE Access*, **8** (2020), 102833–102845. https://doi.org/10.1109/ACCESS.2020.2998725
2. H. Nishida, T. Nguyen, Optimal client-server assignment for internet distributed systems, *IEEE Trans. Parallel Distrib. Syst.*, **24** (2013), 565–575. https://doi.org/10.1109/TPDS.2012.169
3. R. Padilha, F. Pedone, Confidentiality in the cloud, *IEEE Secur. Privacy*, **13** (2015), 57–60. https://doi.org/10.1109/MSP.2015.4
4. C. K. D. S. Rodrigues, V. Rocha, Towards blockchain for suitable efficiency and data integrity of iot ecosystem transactions, *IEEE Lat. Am. Trans.*, **19** (2021), 1199–1206. https://doi.org/10.1109/TLA.2021.9461849
5. J. Seto, Y. Wang, X. Lin, User-habit-oriented authentication model: toward secure, user-friendly authentication for mobile devices, *IEEE Trans. Emerging Top. Comput.*, **3** (2015), 107–118. https://doi.org/10.1109/TETC.2014.2379991
6. L. Lamport, Password authentication with insecure communication, *Commun. ACM*, **24** (1981), 770–772. https://doi.org/10.1145/358790.358797
7. C. L. Lin, H. M. Sun, T. Hwang, Attacks and solutions on strong-password authentication, *IEICE Trans. Commun.*, **E84-B** (2001), 2622–2627.
8. M. L. Das, A. Saxana, V. P. Gulati, A dynamic ID-based remote user authentication scheme, *IEEE Trans. Consum. Electron.*, **50** (2004), 629–631. https://doi.org/10.1109/TCE.2004.1309441
9. Y. Y. Wang, J. Y. Liu, F. X. Xiao, J. Dan, A more efficient and secure dynamic ID-based remote user authentication scheme, *Comput. Commun.*, **32** (2009), 583–585. https://doi.org/10.1016/j.comcom.2008.11.008
10. M. K. Khan, S. K. Kim, K. Alghathbar, Cryptanalysis and security enhancement of a more efficient and secure dynamic ID-based remote user authentication scheme, *Comput. Commun.*, **34** (2011), 305–309. https://doi.org/10.1016/j.comcom.2010.02.011
11. K. Liang, W. Susilo, Searchable attribute-based mechanism with efficient data sharing for secure cloud storage, *IEEE Trans. Inf. Forensics Secur.*, **10** (2015), 1981–1992. https://doi.org/10.1109/TIFS.2015.2442215

12. L. Zhang, J. Zhang, Y. Mu, Novel leakage-resilient attribute-based encryption from hash proof system, *Comput. J.*, **60** (2017), 541–554. https://doi.org/10.1093/comjnl/bxw070
13. C. Lan, C. Wang, H. Li, L. Liu, Comments on attribute-based data sharing scheme revisited in cloud computing, *IEEE Trans. Inf. Forensics Secur.*, **16** (2021), 2579–2580. https://doi.org/10.1109/TIFS.2021.3058758
14. M. Joshi, K. P. Joshi, T. Finin, Delegated authorization framework for EHR services using attribute-based encryption, *IEEE Trans. Serv. Comput.*, **14** (2021), 1612–1623. https://doi.org/10.1109/TSC.2019.2917438
15. J. Sun, H. Xiong, X. Nie, Y. Zhang, P. Wu, On the security of privacy-preserving attribute-based keyword search in shared multi-owner setting, *IEEE Trans. Dependable Secure Comput.*, **18** (2021), 2518–2519. https://doi.org/10.1109/TDSC.2019.2953744
16. Q. Huang, Z. Ma, Y. Yang, X. Niu, J. Fu, Attribute based DRM scheme with dynamic usage control in cloud computing, *China Commun.*, **11** (2014), 50–63. https://doi.org/10.1109/CC.2014.6827568
17. Q. Xu, C. Tan, Z. Fan, W. Zhu, Y. Xiao, F. Cheng, Secure multi-authority data access control scheme in cloud storage system based on attribute-based signcryption, *IEEE Access*, **6** (2018), 34051–34074. https://doi.org/10.1109/ACCESS.2018.2844829
18. Y. Miao, J. Ma, X. Liu, X. Li, Z. Liu, H. Li, Practical attribute-based multi-keyword search scheme in mobile crowdsourcing, *IEEE Internet Things J.*, **5** (2018), 3008–3018. https://doi.org/10.1109/JIOT.2017.2779124
19. S. Zhu, L. Zhan, H. Qiang, D. Fu, W. Sun, Y. Tang, A fuzzy attribute-based authentication scheme on the basis of Lagrange polynomial interpolation, in *Proceedings of International Conference on Human Centered Computing (HCC'14)*, (2014), 685–692. https://doi.org/10.1007/978-3-319-15554-8_57
20. J. P. Yun, H. Kim, D. H. Lee, An improved fuzzy attribute-based authentication, in *Proceedings of 2015 5th International Conference on IT Convergence and Security (ICITCS'15)*, (2015), 1–5. https://doi.org/10.1109/ICITCS.2015.7292946
21. H. Y. Lin, P. Y. Ting, H. R. Wu, An attribute-based mutual authentication scheme with time-bounded keys, in *Proceedings of the 2019 the 3rd International Conference on Telecommunications and Communication Engineering (ICTCE 2019)*, (2019), 75–79. https://doi.org/10.1145/3369555.3369568
22. J. Hao, J. Liu, H. Wang, L. Liu, M. Xian, X. Shen, Efficient attribute-based access control with authorized search in cloud storage, *IEEE Access*, **7** (2019), 182772–182783. https://doi.org/10.1109/ACCESS.2019.2906726
23. Y. Xie, H. Wen, B. Wu, Y. Jiang, J. Meng, A modified hierarchical attribute-based encryption access control method for mobile cloud computing, *IEEE Trans. Cloud Comput.*, **7** (2019), 383–391. https://doi.org/10.1109/TCC.2015.2513388
24. S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay, J. J. P. C. Rodrigues, Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications, *IEEE Trans. Ind. Inf.*, **15** (2019), 457–468. https://doi.org/10.1109/TII.2018.2824815
25. J. Hong, K. Xue, Y. Xue, W. Chen, D. S. L. Wei, N. Yu, et al., TAFC: time and attribute factors combined access control for time-sensitive data in public cloud, *IEEE Trans. Serv. Comput.*, **13** (2020), 158–171. https://doi.org/10.1109/TSC.2017.2682090

26. H. Ma, R. Zhang, S. Sun, Z. Song, G. Tan, Server-aided fine-grained access control mechanism with robust revocation in cloud computing, *IEEE Trans. Serv. Comput.*, **15** (2022), 164–173. https://doi.org/10.1109/TSC.2019.2925028
27. A. Candan, An efficient filtering structure for Lagrange interpolation, *IEEE Signal Process Lett.*, **14** (2007), 17–19. https://doi.org/10.1109/LSP.2006.881528
28. Z. Ergul, I. Bosch, L. Gurel, Two-step lagrange interpolation method for the multilevel fast multipole algorithm, *IEEE Antennas Wirel. Propag. Lett.*, **8** (2009), 69–71. https://doi.org/10.1109/LAWP.2008.2011063
29. S. D. Galbraith, K. G. Paterson, N. P. Smart, Pairings for cryptographers, *Discrete Appl. Math.*, **156** (2008), 3113–3121. https://doi.org/10.1016/J.DAM.2007.12.010
30. R. C. Márquez, A. J. C. Sarmiento, S. Sánchez-Solano, Implementing cryptographic pairings on ARM dual-core processors, *IEEE Lat. Am. Trans.*, **18** (2020), 232–240. https://doi.org/10.1109/TLA.2020.9085275
31. J. S. Balakrishnan, A. Besser, Computing local p-adic height pairings on hyperelliptic curves, *Int. Math. Res. Not.*, **2012** (2012), 2405–2444. https://doi.org/10.1093/imrn/rnr111

AIMS Press