Journal of New Media
DOI:10.32604/jnm.2020.09946
Article

Tech Science Press

Authorized Attribute-Based Encryption Multi-Keywords Search with Policy Updating

Muqadar Ali, Chungen Xu* and Abid Hussain

Department of Mathematics, School of Science, Nanjing University of Science and Technology, Nanjing, 210094, China
*Corresponding Author: Chungen Xu. Email: xuchung@njust.edu.cn
Received: 03 February 2020; Accepted: 08 February 2020

Abstract: Attribute-based encryption is cryptographic techniques that provide flexible data access control to encrypted data content in cloud storage. Each trusted authority needs proper management and distribution of secret keys to the user's to only authorized user's attributes. However existing schemes cannot be applied multiple authority that supports only a single keywords search compare to multi keywords search high computational burden or inefficient attribute's revocation. In this paper, a ciphertext policy attribute-based encryption (CP-ABE) scheme has been proposed which focuses on multi-keyword search and attribute revocation by new policy updating feathers under multiple authorities and central authority. The data owner encrypts the keywords index under the initial access policy. Moreover, this paper addresses further issues such as data access, search policy, and confidentiality against unauthorized users. Finally, we provide the correctness analysis, performance analysis and security proof for chosen keywords attack and search trapdoor in general group model using DBDH and DLIN assumption.

Keywords: Attribute-based encryption; access control; multi-keywords search; policy updating

1 Introduction

Reflecting on the new trend and repaid development in information technology and the Internet of Things (IoT) a large amount of data is generated and related to our lives. For such kind of large data, cloud computing enables us to share, access, and save these data for saving costs. Along with such facilities, there are many threats and issues such as data storage, data processing, data accessing, and data search. Where different parties would like to share their data for user's attributes to access and achieve hidden access policy. Traditionally, the outsource data usually encrypted to find out a significant access control technique to achieve fine-grained access control i.e., attribute-based encryption (ABE) can be classified into two categories one is KP-ABE key policy attribute-based encryption in which secret key is attached to the access policy and ciphertext attached to the attribute set. The other one is CP-ABE ciphertext policy attribute-based encryption in CP-ABE a secret key is attached to attribute set and ciphertext attached to access policy. Li et al. [1] proposed a scheme that combines both CP-ABE ciphertext policy attribute-based encryption and KP-ABE key policy attribute-based encryption an application scenario of personal health records (PHR) where the users are divided into public and personal domain according to their roles. Meng et al. [2] proposed a key policy attribute-based encryption scheme using the prime order group to show the scheme efficiency. In CP-ABE scheme of Bethencourt et al. [3] which is public-key cryptography that resolves the issue of fine-grained access control of shared data. In Cheng et al. [4] proposed a CP-ABE scheme for a large universe of attributes set, which reduces the storage and computational overhead of the existing CP-ABE scheme. Since the existing scheme cannot support the multi-keywords search, in order to address this problem Miao et al. [5] proposed the

ABE scheme personal health records with multi-keywords searches directional application for searchable encryption. Liu et al. [6] proposed the CP-ABE scheme multiple attribute authority with a central authority. But the scheme overall performance is low and the central authority has a security bottleneck in large distributed systems. However, in CP-ABE user's revocation is flexible and challenges to revoke partial access users privilege for his/her attributes. Liu et al. [7] presented an ABE scheme contains both outsource decryption, attribute revocation to set of the random number of each attribute to perform an efficient revocation, but the design scheme does not support keywords search.

1.2 Related Work

It is necessary for the data owner a primitive hidden and fine-grinned data access control issue which pave the way to perform flexible keyword search control by using promising attribute-based encryption for specific access policy. That why Sun et al. [8] proposed an ABE keywords searchable encryption scheme for the implementation of fine-grained access control for encrypted data because of attribute-based encryption implementation is extensive and flexible with access policy. Whereby using (ABE-KS) attribute-based encryption keywords search the computation and communication costs are linear to the number of existing attributes in the scheme. The Zheng et al. [9] arose the notion of attribute-based keywords search in which data owner is enabled to set the access policy for the data users to search on the encrypted data only if their attributes satisfy the data owner access policy. Li et al. [10] presented ABE scheme for the verifiable outsources decryption with full verifiability for the outsource decryption verification scheme which is used in the correctness verification transformation of ciphertext checking access authorization of certain users and the scheme selective CPA secure in the standard model. Wang et al. [11] proposed a traceable attribute-based encryption scheme to detect a malicious authorized user who leaks key during data sharing and support revocation. Where the number of operations in the decryption process depends on the complexity of the scheme policy used with limited computing power. However, the most urgent problem in nowadays is how to reduce the user's computational load with specific limited time to achieve effective keywords, search. Several CP-ABE likes Wang et al. [12,13] schemes had been proposed to access the encrypted data and perform fine-grained data access control. Yin et al. [14] presented an efficient ciphertext policy attribute-based encryption scheme that supports AND/OR gate and threshold gate. However, the query keyword in the scheme is vulnerable against the chosen-plaintext attack and the search token generation algorithm is deterministic encryption. Where Li et al. [15] proposed an attribute-based encryption scheme for multi-authority to provide security proof against chosen-ciphertext attacks and also supports attribute revocation. Li et al. [16] presented an ABE scheme to achieve keywords search for the outsource encrypted data but the scheme cannot support attribute revocation. Since Wang et al. [17] recently proposed for a verifiable ABE scheme to perform a multi-keywords search, data outsourcing and verifiability of outsourcing a private key but the scheme cannot achieve the user's attribute's revocation. Guo et al. [18] design a constant ciphertext size CP-ABE scheme for the key storage in lightweight devices to define an expressive access policy for the user's attributes. The Liu et al. [19] propose an efficient practical CP-ABE scheme to performs both attribute revocation, outsource decryption, and policy updating. We focus in this paper multiple authorities, multi keywords search and efficient user's attribute's revocation with policy updating to performs fine-grained access control with low computation burden on client-side.

1.3 Challenges and Our Contribution

In this paper, we design (CP-ABE) comprehensive scheme that is used to solve many issues and state that our scheme supports simultaneously a) multiple authorities b) large attribute universe c) multi keywords search d) user's attribute's revocation e) policy updating.

1) We proposed multiple authorities secure (CP-ABE) scheme for multi keywords, search compare to single keywords search under the hidden access policy of encrypted data to the cloud server. The only authorized user's attributes are allowed to search the interesting keywords, decryption of ciphertext correctly using access rights of initial access policy and policy updating process by the data owner.

2) The define CP-ABE scheme provides a secure transformation of the secret keys to users and data owner through each trusted attribute authorities with a low computation burden.

3) The proposed multiple authorities (CP-ABE) scheme needs verification to gives better security proof in the existence of the central authority further the user's attribute's revocation the number of all non-revoked user's attribute's keys and revoked user's attributes related ciphertext can be updated through a new access policy generate new index set such that data user whose attribute is revoked does not decrypt an updated ciphertext with the previous key, our scheme resists against to prevent collision attack with different global identity to preserve ciphertext policy.

4) Our scheme is provably secure under the standard model that formulate a reasonable security model and provide formal security proofs for chosen keywords and search trapdoor.

The rest of this paper is organized as follows.

The preliminaries definition of our scheme construction in Section 2. The system model and security model are describing in Section 3. Scheme concrete construction and security proof for chosen keywords attack (CKA) and search trapdoor proven in Sections 4 and 5. The details of correctness analysis proof, theoretical, and performance comparison analysis are shown in Section 6. Finally, we have drawn and conclude the paper in Section 7.

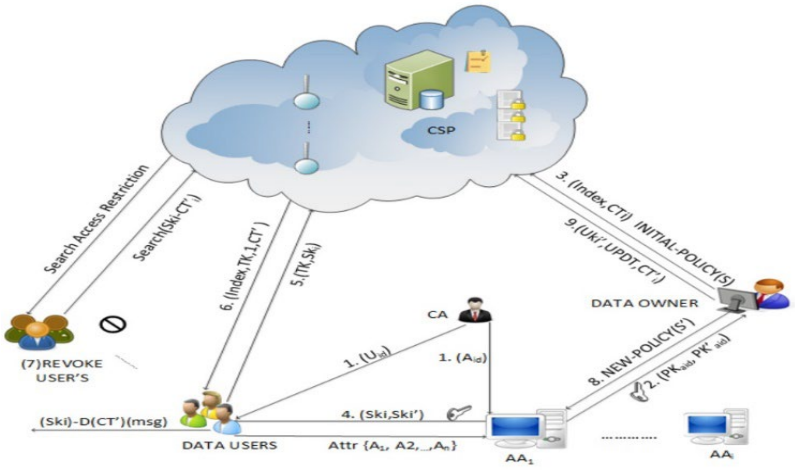

Figure 1: System model

2 Preliminaries

In this section, we review some basic cryptographic definitions Bilinear maps, Decisional Linear assumption (DLIN) Access Structure, and Linear Secret Sharing Scheme as follows.

2.1 Bilinear Maps [20]

Defination 1: Bilinear maps:

Let $\mathbb{G}$, $\mathbb{G}_T$ be two multiplicative cyclic groups with prime order p and g is a generator of the group $\mathbb{G}$. let e: $\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ be bilinear map satisfies the following properties.

1) Bi-linearity 2) Non-degeneracy and 3) Computability.

2.2 (DLIN) Decisional Linear Assumption [21]

Defination 2: Decisional Linear assumption:

An asymmetric group generator Group-Gen satisfies the decisional linear assumption (DLIN) for all PPT adversaries $\mathcal{A}$ and the advantages of $\mathcal{A}$ as follow.

$ADV^{A}_{DLIN(\eta)} = \Pr[\mathcal{A}(1^{\eta}), Par, D, R_0 = 1] - \Pr[A(1^{\eta}), Par, D, R_1 = 1]$ is negligible in security pram η where $Par = (g, h, H, \mathbb{G}, \mathbb{G}_T)$, $D = \left(h, g^{a}, g^{b}, g^{r_1}, g^{r_2}, h^{r_1+r_2}, g^{r_1+r_2}\right)$ $a, b \in \mathbb{Z}_p^*$ and $r_1, r_2, r \in \mathbb{Z}_p$,$R_0 := (g^{r_1+r_2}, h^{r_1+r_2})$;$R_1 := (g^{r}, h^{r})$.

2.3 Access Structure [18]

Defination 3: Access structure:

Let $\mathbb{A} = \{A_i\}_{i=1\ldots n}$ be the set of attributes a collection $\mathbb{S} \subseteq 2^{\{A_1, A_2, \ldots, A_n\}}$ is monotonic $\forall B, C$ if, B$\in$ $\mathbb{S}$, B$\subseteq$ C then $C \in \mathbb{S}$. An access structure is a collection $\mathbb{S}$ of a non-empty subset i.e., set $\mathbb{S} \subseteq 2^{\{A_1, A_2, \ldots, A_n\}}$. We mean a monotonic access structure the set in $\mathbb{S}$ is called authorized set where the set not in $\mathbb{S}$ is called an unauthorized set. The access structure can be converted into a Boolean function. The Boolean function works as an access tree the attribute set present in leaf nodes the intermediate and root nodes of an access tree are the logical operator AND/OR gate.

2.4 Linear Secret Sharing Scheme [19]

Defination 4: (LSSS) Linear secret sharing scheme:

A linear sharing scheme over a set of attributes $\mathbb{A} = \{A_i\}_{i=1\ldots n}$ is called linear over $\mathbb{Z}_p$ with l row and n column that called the sharing generating matrix of Π with $\forall i$=1,…, l of matrix M. We let a function ρ define the attributes labeling row of a matrix M to i attributes is (ρi). Where we consider column vector $v = (s, r_1, \ldots, r_n)^T$ and $s \in \mathbb{Z}_p$ is a share of a secret to be shared. Chosen randomly $r_1, \ldots, r_n \in \mathbb{Z}_p$ then $(Mv)i$ is l share of secret s according to Π. The share (Mv) is belong to attributesA_i. According to the linear reconstruction property of Π is (LSSS) for the matrix M of an access structure $\mathbb{S}$. Where $A_i \in \mathbb{S}$ be authorized attributes set and let $I \subset \{1,2,..l\}$ can be defined as $I = \{i: (\rho i) \in A_i\}$ there exist $\{\lambda_i \in \mathbb{Z}_p\}, i \in I$ mean polynomial time in the size of a matrix if, (λ_i) is valid share secret according to Π. And $s = \sum_{i \in I} \gamma_i \lambda_i$ otherwise for the unauthorized set, no such constant is existing.

3 System Model Definitions Overview and Security Model

In this section, we provide a system model, access control framework and our security model for our proposed CP-ABE scheme under policy updating.

3.1 System Model

As shown in Fig.1 our CP-ABE scheme with keywords and attribute's revocation in the existing central authority, multiple authorities, cloud server, data owner and the multi user's for large attribute universe consists of the following five entities.

1) Central-Authority (CA): The CA is a trusted certificate authority responsible for both the users and each attribute authority registration, user's authentication to reduce security issues like correctness fraud error. Note that it does not participate in any kind of the attribute's related operation.

2) Attribute-Authority (AA): Each attribute authority (AA_i) is a trusted authority that is responsible for system initialization, secret key generation, and distribution to the user's attribute, according to the user's rule or identity. During revocation of users attributes each attribute authority (AA_i) update the secret keys of non-revoked users and data owner under the secure channel.

3) Cloud-Service-Provider (CSP): The (CSP) provide the data storage for the data owner and data access service for the data users. It provides search facilities on encrypted keyword index and ciphertext if, the matching succeeds to users request it, send the ciphertext, and searched keywords to respective users otherwise deny. The CSP updates the ciphertext after the attribute's revocation based on updated keys.

4) Data-Owner (DO): The (DO) first defines the access policy for the set of users attributes symmetrically encipher the data under hidden access policy upload the keyword search index along with ciphertext to CSP. Only those data users will be able to search and decrypt the uploaded index that

satisfies the access structure embedded in the ciphertext. The data owner creates a new attribute users index set under a new access policy in revocation phase.

5) Data-Users (DU): The (DU) is an authorized set in which each user identifies with a unique identity uid and certificates that satisfy the access structure embedded in the ciphertext. The data users generate search token and send to CSP while CSP compare the token with keywords query to the encrypted index and successful return search result in an interesting keyword search $\tilde{w}_{m'}$ to respective attributes, users satisfy the access structure of access policy.

3.2 High Level Overview

In our scheme, there is the n number of attribute authorities $AA_i = \{AA_1, AA_2, \dots, AA_n\}$ each authority manages a set of attributes $\mathbb{A} = \{A_i\}_{i=1,\dots n}$ and choose randomly $\alpha, \beta \in \mathbb{Z}_p^*$ for $i \in [A_i]$ and α for the attributes revocation. Generate the public-key as $g^{\alpha b}$ the attribute set embedded in the ciphertext with a public key PK. In order to resolve the issue of collision resistance to create a secret key for the user's using GID to relative attributes A_i the authority (AA_i) first, compute $(x_i, y_i) = \prod_{i\in I} \tilde{p}.U_i$ then authenticate the certificate $sig\mathrm{CA}_{\mathrm{sk}}$. If, any user combing their secret key component using different global identities can appear in the form of $(GID, e(g,g)^{\alpha\beta\tilde{p}_i r_i \sum_{i\in I}\lambda_i\gamma_i})$ otherwise, it can be traced during the process of decryption $(HGID^*, e(g,g)^{\alpha\beta\tilde{p}_i^* r_i \sum_{i\in I}\lambda_i\gamma_i})$ using different global identities we can prevent collision resistance in this way. The keywords index and ciphertext policy can be protected using a random number chosen $\theta \in \mathbb{Z}_p^*$ by the data owner encrypting the keywords index $\tilde{u} = g^{\theta}\prod_{j=1}^{m'} U_i$ as along with ciphertext choose $r_i, \lambda_i, s_i \in \mathbb{Z}_p$ and compute $C = Enkg^{\tilde{p}_i\beta\alpha r_i s}$ hence the privacy policy can be implemented that preserved in the access policy. In the process of the user's attribute's revocation, the central authority issues the list of revoke user's send to each authority to update the secret key for the user's attribute in the system. The data owner defines a new access policy to update and generates a new attribute user's index.

3.2 Security Model

The cloud server executes the operation on encrypted data but the server is also curious about the encrypted data content. However, we define the security model for our CP-ABE scheme under central authority none adaptive security game procedure between the $\mathcal{C}$ and Adversary $\mathcal{A}$ and allow the $\mathcal{A}$ with corrupt authority AAC a certain set of attribute authorities (AA_i) by getting the system parameter and send the entire queries to the challenger $\mathcal{C}$ as follow.

(Adversary Queries) The Adversary submit his queries choose a random bit $b' \in (0,1)^*$ to the $\mathcal{C}$ as authorities $(AA_i - \mathrm{AAC})$ remaining authorities are corrupt. The advantages of $\mathcal{A}$ to win the game successfully show in the end the $\mathcal{C}$ flip a random bit $b \in (0,1)$ reply to the adversary queries.

a) (Setup)CA-Setup$(1^{\eta}) \rightarrow (sp, CA_{PK}, CA_{sk})$ The $\mathcal{C}$ run the setup algorithm for CA all corrupt authorities (AAC) to obtain the public key, a master key by giving the public key to the $\mathcal{A}$ and kept the master key secret. The corrupt authority for which adversary query on $A_i^* \subseteq A_i$ to issues public-key query.

b) (AA-Public-Key) The adversary makes a query for none corrupt authority public key (APK_{Aid}) as $APK_{Aid} = AA_i - \mathrm{AAC} = \mathrm{AuthN}$ by himself and send it to the challenger. For non-corrupt authority AuthN the $\mathcal{C}$ send the public key to the $\mathcal{A}$ and keep master key, secret.

c) (Secret-Key-Query) $(APK_{Aid}, S^*, A_i^*, M_{SK}^*, sp^*, SK^*, sig(CA_{SK}u_{id}^*)) \rightarrow (SK_i^*)$ Adversary makes a secret key query for the corrupt authority with pairs of keys, challenge access policy and system parameter with the illegal certificate registers from CA which does not issue secret key for the A_i^* entitled as unauthorized attributes. Because $\mathcal{A}$ create the secret key as the difference $(AA_i - \mathrm{AAC})$ so for corrupt AAC the $\mathcal{A}$ create $(HGID^*, SK_{idi}^*)$ query by himself and submit to the challenger. The $\mathcal{C}$ reply on $\mathcal{A}$ access policy $S^*$and run a secret key generation algorithm with the query $uid \neq uid^*, A_i \in S$ because $\mathcal{C}$ authenticate and verify the certificate that does not exist in the list of legal users. Where GID^* is an illegal

global identity for A_i^* are the unauthorized attributes of $\mathcal{A}$ to attribute authority which cannot satisfy himself as a non-corrupt authority.

d) (Keyword-query) Adversary $\mathcal{A}$ select an access policy S_b^*=S_1^*,S_0^* for selected keywords with access structure $\tilde{p}_i^*$ and $\tilde{w}_{Lmb}^*$=$\tilde{w}_{0,Lm}^*$,$\tilde{w}_{1,Lm}^*$ for A_i^* if, $\gamma(A_i^*, S_0^*) = 0 \wedge \gamma(A_i^*, S_1^*)$=0 not satisfied the adversary $\mathcal{A}$ get SK_{idi}^* otherwise, terminate. The adversary chooses another query keyword set $\tilde{w}_{m'}^*$ with $\tilde{p}_i^*$ for $\tilde{w}_{m'}$ send to the challenger $\mathcal{C}$. Finally, the Challenger replies with the keyword encrypt algorithm for $\mathcal{A}$ chosen keywords set $\tilde{w}_{Lm}^*$ and $\tilde{w}_{m'}^*$. The adversary cannot be longer queried for the authorized and legitimate keywords index $\tilde{w}_{Lm}$ and $\tilde{w}_m$ because $\mathcal{A}$ does not satisfy himself as a non-corrupt authority.

e) (TK-Query) For the chosen keyword set $\tilde{w}_{m'}^*$ the adversary $\mathcal{A}$ run the token generation algorithm for attribute's set which cannot match to the legitimately interested keywords set $\tilde{w}_{m'}$ of the data owner. Challenger reply to run Key-Gen algorithm on the public key, secret key, keyword set $\tilde{w}_{m'}^*$ and S^* submit by $\mathcal{A}$ and $\mathcal{C}$ restrict A_i^* with $\tilde{p}_i^*, S^*$does not satisfies the access policy S the challenger $\mathcal{C}$ generates a token for the keywords set $\tilde{w}_{m'}^*$ and send to the adversary.

(Guess): The advantage of an adversary $\mathcal{A}$ in the above game output guess b_0 of b' with negligible probability.

$Prob[b_0=b'] - \frac{1}{2}$

4 An Authorized Attribute-Based Encryption Multi Keywords Search with Policy Updating

In this section, we describe the concrete construction of our CP-ABE including multiple user's attribute revocations with policy updating consist of the following eleven algorithms.

4.1 System Setup and Access Control Framework

In this, the system initialization consists of two main algorithms one is central authority (CA) setup and another one is an attribute authority (AA_i) setup as shown below.

1) CA-Setup(1^η) → (sp, CA_{PK}, CA_{sk}) The central authority (CA) input the security parameter η and output system parameter sp , central authority public key and secret key. Choose $a \in \mathbb{Z}_p$ and compute $sp = g^a$ the central authority registered both of the (AA_i) and users (U_i) as follow.

2) Registration $(Aid, CA_{sk}, U_i) \rightarrow (PK_{CA}, sp, PK_{uid}, GID, sigCA_{sk}(u_{id}))$ The Central authority taking each authority identity along with its secret key for all legal authority and users who want to join in the system. Randomly choose $a, r \in \mathbb{Z}_p$ to return its public key PK_{CA} system parameter sp for (AA_i). The CA first, assign users with global identity GID generates the public key $PK_{uid} = g^{a_{uid}}$ and issues certificate using its secret key $sig\mathrm{CA_{sk}} = (HGID, u_{id}, g^{\frac{1}{ruid}})$ to each user.

3) AA-Setup$(sp, A_i, Aid) \rightarrow (PK_{Aid}, M_{SK})$ The attribute's authority (AA_i) taking security parameter, an attribute's set with respective attribute authority identity and output public key and master secret key. Using a bilinear map e: $\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ of a group $\mathbb{G}$ prime order p with generator g and hash function $\mathbb{H}(0,1) \rightarrow \mathbb{Z}_p^*$ choose $a, b, c \in \mathbb{Z}_P$. Using Lagrange interpolation formula $\Delta a_{(xi)} = \prod_{j \in a(x) i \neq j} [\frac{x-j}{i-j}]$ with interpolation coefficient $a(xi)$ denote $(i, j) \in \mathbb{Z}_p^*$ choose $\alpha, \beta \in \mathbb{Z}_p^*$ compute $PK_{Aid} = Y = e(g, g)^{\alpha b}$ $AU_i = g^{-r_i \tilde{p}_i}$ return public keys for the set of users attributes (x_i, y_i) under in access structure. Randomly choose $(r_1, r_2, .., r_n)$ and $(s_1, s_2, .., s_n)$ for the set of authorized users attributes and publish the public keys and master secret key as $PK = (g, \mathbb{G}, e, \mathbb{G}_T, g^{\alpha b}, Y, \mathbb{H}, \{PK_{Aid}\}, i \in [1, n]$ and $M_{SK} = (\alpha, \beta, x_i, y_i), g^\alpha, g^c, i \in [1, n])$.

4) Key-Gen$(PK_{Aid}, S, A_i, M_{SK}, sp, sigCA_{sk}(u_{id})) \rightarrow (SK, SK_i, SK_{idi})$ The AA_i input the public key, access policy, attributes set, master secret key, system parameter, and user's certificate output outsource private key, content key, and secret key for each legal user. First, compute $\tilde{p} = g^\alpha$ and for each $U_i \in$

$[1,n]$ n number of users verify the access structure $\tilde{p}$ of access policy for users attribute set x_i, y_i as shown in Eq. (1.1).

$$(x_i, y_i) = \prod_{i\in I} \tilde{p}.AU_i \tag{1.1}$$

Randomly choose w, $r_i, \lambda_i \in \mathbb{Z}_p$ check $y_i^w = \prod_{i\in I} e(g, g^{-\alpha r_i})^{w\tilde{\mathrm{p}}_i}$ and $x_i{}^w = \prod_{i\in I} e(g, g^{-\alpha r_i})^{w\tilde{\mathrm{p}}_i}$ if the access policy satisfies for the access structure $\tilde{\mathrm{p}}_i$ returned the outsource secret key $SK = (\tilde{\mathrm{p}}, x_i, y_i), A_i \in S$. To generate secret key each AA_i first, authenticate the user to check the legality and verify the certificate $sig\mathrm{CA}_{\mathrm{sk}} = \left(HGID, u_{id}, g^{\frac{1}{ruid}}\right)$. If the user is legal each AA_i assign users to related attributes. For the authorized attributes it computes $D_{(\pi)i,1} = g^{(u-\beta-\gamma_i)}$ $D_{(\pi)i,2}$=$g^{(\alpha u-\gamma_i)}$ π is map each user attribute set, output content key for an encrypted message SK_{idi}=$\{ D_{(\pi)i,1}, D_{(\pi)i,2})\}, i \in [1,n]$. The authority using global identity GID of users randomly choose a, b, r_1, $r_2 \in \mathbb{Z}_p$ for $A_i \in \mathbb{A}$, $i \in [1,n]$ generate the secret key using global identity for a group of user's as $SK_i = HGIDg^{\tilde{\mathrm{p}}_i(u+r_i)}$.

5) Encryption$(PK_{aid}, S, CT_i, \widetilde{\mathrm{w}}_{Lm}, \widetilde{\mathrm{w}}_{m'}) \rightarrow (|Index|)$ The data owner first symmetrically encrypts the data on the rely of the encryption key input the attribute authority public key, access policy, encrypted ciphertext, keywords search index, search query keywords. Output the index set and upload to the CSP. The access policy $S = (M, \rho)$ where ρ is a map each M_i of matrix M to attributes set (ρi). Randomly choose r_1 ,…, $r_n \in \mathbb{Z}_p$ and two random vectors as $\upsilon = (s, \upsilon_1, \upsilon_2, \dots, \upsilon_n)^T$ and $\mu = (0, \mu_1, \mu_2, \dots, \mu_n)^T$ compute $\lambda_i = M_i\upsilon$, $\gamma_i = M_i\mu$. Computes the keywords search index, choose $b, r_1, r_2 \in \mathbb{Z}_p, I_{wj} = g^{\theta}$: $\widetilde{\mathrm{w}}_{m'} = g^{bc\theta}$; $\widetilde{\mathrm{w}}_{Lm}$=$g^{b(r_1+r_2)}g^{H\left(w_j'\right)} \in \mathbb{G}, j \in [1,m]$, $\widetilde{\mathrm{w}}_{Lm}L \in [1,m]$ with access structure $\tilde{p}_i$. The data owner encrypts the keywords index for the user's attributes shown in Eq. (1.2) with access policy $S = \{Attr(x_1, x_2 \dots, \wedge, \dots, x_i)\} \vee \{Attr(y_1, y_2 \dots, \vee, \dots, y_i)\}$.

$$\tilde{\mathrm{u}} = g^{\theta} \prod_{j=1}^{m'} U_i \in \mathbb{G}_T \tag{1.2}$$

Randomly choose $r_i, \lambda_i, s_i \in \mathbb{Z}_p$, $\alpha, \beta, \theta \in \mathbb{Z}_p^*$ compute the ciphertext $C = Enkg^{\tilde{\mathrm{p}}_i\beta\alpha r_i s}$, $C_1 = g^{\lambda_i}$, $C_{i,1} = e(u_i)^{s_i}$, $C_{i,2} = x_i^{s_i}$ $C_{i,3} = y_i{}^{r_1\lambda_1}$ and output overall ciphertext $CT_i = (\tilde{p}_i, CT', C, C_{i,1}, C_{i,2}, C_{i,3}) \in \mathbb{G}$. Finally, the data owner returns the keywords index under the access structure as follow $|Index| = (\tilde{p}_i$, $\{\widetilde{\mathrm{w}}_{Lm}, \widetilde{\mathrm{w}}_m\}, CT_i, Enk(msg), CT')$.

6) Gen-TK$(PK_{uid}, S, SK_i, \widetilde{\mathrm{w}}_{m'}) \rightarrow (TK_i)$ Each user inputs its public key, access policy, secret key, search query keyword index $\widetilde{\mathrm{w}}_{m'}$ the authorized users verify the access policy if search token matches the secret key of users CSP successfully return TK_i , $i \in [1,n]$ for $i \in S$, $A_i \in \tilde{p}_i$, . Randomly choose $b, c, r_i \in \mathbb{Z}_p$ generates the search token as $TK_i = (TK_1, TK_2, TK_3)$ where return tokens $TK_1 = \prod_{j=1}^{m'}(g^{bcr_1}g^{bH\left(w_j'\right)})$, $TK_2 = g^{b\theta}, TK_3 = g^{r_2}$.

7) Search $(|Index|, TK_i, \widetilde{\mathrm{w}}_{m'}) \rightarrow (1, \perp)$ The users can search send TK_i in interested query keyword $\widetilde{\mathrm{w}}_{m'}$ to CSP. For search $TK_{\boldsymbol{i}}$ server make a check if, the keyword index can match to the search TK_i the CSP output 1 to transmit the keywords to users must satisfy the following Eq. (1.3).

$$Search(w_j')= e\left(\prod_{j=1}^{m'}(\widetilde{\mathrm{w}}_{Lm}, TK_2\right) = e\left(I_{wj}, TK_1\right)e(\widetilde{\mathrm{w}}_{m'}, TK_3) \tag{1.3}$$

The data owner encrypts m keywords as $\tilde{\mathrm{u}} = g^{\theta}\prod_{j=1}^{m'} u_i \in \mathbb{G}_T$ generate an index set I_{wj}. The keywords index $w_{Lm} = L \in [1,m]$ is a set of extracted keywords from files. Using statistical probability formula to execute the number of selected query keywords to the number of total query keywords.

$$C_L^{m'} = \frac{L(L-1)(L-2),\dots(L-m'+1)}{m'!} \tag{1.4}$$

Total number of randomly selected keywords the CSP match index set probably if Eq. (1.4) verify. Only there is at least one keywords match the search token of search query keywords the CSP successfully return 1 otherwise $\perp$.

8) Decryption $(PK, SK_i, CT') \rightarrow (msg)$ The DU using a content key SK_{idi} to decrypt the CT'successfully output 1 if any user satisfies the access policy of access structure embedded in ciphertext otherwise, 0. The CSP deny for unauthorized user's attributes and output 0. According to LSSS property if λ_i are valid share for secret s there exist such constant $\{\lambda_i \in \mathbb{Z}_p\}, i \in I$ the algorithm first calculate $s = \sum_{i\in I} \gamma_i \lambda_i$ to recover secret share. The decryption is successful verify using a content key only if , $A_i \in \tilde{p}_i$ $\gamma(A_i, S) = 1$ $i \in S$ and $i \in [1, n]$ of authorized attribute's return correctly match encryption key with the ciphertext $CT_i = \frac{msg}{Enk} = (Enk)CT_i = msg$ satisfy the Eq. (1.5).

$$Enk(CT_i) = \frac{msg(e(C\prod_{i\in I} C_{i,1}, D_{(\pi)i,2})}{e(\prod_{i\in I} e(C_{i,2}, D_{(\pi)i,1})} \tag{1.5}$$

4.2 Policy-Updating [19]

Our CP-ABE scheme for attribute's user's data owner dynamically updated the policy to achieve an efficient revocation by the following main three algorithms.

9) Attribute's-Users-Index-Update 10) Key-Update 11) Ciphertext-Update.

9) Attribute's-Users-Index-Update $(RA_i, PK'_{Aid}, M'_{SK}, \tilde{p}_{i'}, S', S, GID^*) \rightarrow (RA_{i'}, I_{M'})$

The data owner generates a new user's index set of non-revoked users attribute send to attribute authority input revoke user's attributes updated public key, master key, global identity, and initial access policy/new access policy. Output $RA_{i'} = (i, j) - (0, j)$ remove the corresponding user's attribute's I_M=$\{(M, \rho)_{(i,j)\in l\times n}(i, j)\}$ from none updated index $I_{M'}$=$\{(M', \rho')_{(i,j)\in l'\times n'}(0, j)\}$ to generate new Index. Choose two random vectors $v' = (s, v'_1, v'_2, \dots, v'_n)^T$ and $\mu' = (0, \mu'_1, \mu'_2, \dots, \mu'_n)^T$ compute $\lambda'_i = M'_i v'$, $\gamma'_i = M'_i \mu'$. If $(i, j) \in I_M$ then $(0, j) \in I_{M'}$ are the newly updated index set for the non-revoke user's attribute's generated by the data owner. Let $S = (M, \rho)$ and $S' = (M', \rho')$ represent an initial access policy/new access policy to generate a new index set by the following algorithm operation on a matrix M of size $l \times n$.

i) Input $S = (M, \rho)$ and $S' = (M', \rho')$

ii) adding (i, j) remove i attribute's from I_M while output $I_{M'}$

iii) where $I_M \neq \phi \; \exists \; i \in M$ until do ρ==ρ'

iv) Output $I_{M'}$ new index set of row index $M' = l' \times n'$

v) return $I_{M'}$

vi) End If

10) Key-Update $(RA_{i'}, PK'_{Aid}, M'_{SK}, S') \rightarrow (UK_{i'})$ In attribute users revocation each AA_i input un-revoke attributes updated index, public key, master key, new access policy updating keys for non-revoked user's attributes. Randomly choose $z, a_i, \lambda'_i, r'_i, \gamma'_i \in \mathbb{Z}_p$ and $\alpha', \beta' \in \mathbb{G}$ return public key PK'_{Aid} , master key M'_{SK} computes $\tilde{\mathrm{p}}' = g^{\alpha'}$ while update keys $UK_{i'} = g^{(\alpha'_i - \alpha_i)}, (i \in I'_M, GID)$. The AA_i first, update the outsource private key $SK' = e(g, g)^{z\tilde{p}'_i(\alpha'_i - \alpha_i)} = (\tilde{p}', x_i, y_i)$ using the outsource private key the attribute authorities update content key

$SK'_{idi} = (\forall i \in I'_M, GID \setminus GID^*) = D'_{(\pi)i,1} = g^{(a_i - \beta' - \gamma'_i)}$, $D'_{(\pi)i,2}$=$g^{(\alpha' a_i - \gamma'_i)}$.

Then update the secret key $UK_{i'} = SK'_{idi} = HGIDg^{(a_i + r'_i)}$ of non-revoked users, attribute's under new access policy S' while the identity of the revoke users will be deleted from the system.

11) CT-Update $(RA_{i'}, CT_i, UK_{i'}, S') \rightarrow (CT'_i)$ The DO input non-revoke users list $RA_{i'}$ get the updated key $UK_{i'}$ from the AA_i collection the i^{th} block of ciphertext CT_i under new access policy S'. Update those components of ciphertext related to revoke user's attributes. Choose randomly $a_i, \lambda'_i, r'_i, k'_i \in \mathbb{Z}_p, \alpha', \beta' \in \mathbb{G}$ compute and update ciphertext.

$\forall i = 1 \; to \; m \; if: \rho(i) \in (I_M, GID), \; CT'' = CT' = CT \cdot g^{r_1 + r_2} = e(g, g)^{\rho'_i(\alpha - r'_1 r'_2)}$

$C' = C = e(g,g)^{\tilde{p}_i'\beta\alpha r_i s} = e(g,g)^{a_i\alpha'\beta'\lambda_i'}, C_{i,1}' = (C_{i,1})^{s_i} = e(U_i)^{s_i} = e(g,g)^{\lambda_i'}$

$C_{i,2}' = e(x_i)^{s_i} = e(g,g)^{a_i\lambda_i'}$ Repeat until ρ==ρ', $\rho_i' \in (I_M', GID \setminus GID^*)$ ciphertext

$CT_i' = CT_i$ output the i^{th} block of updated ciphertext $(CT_i') = (\tilde{p}_i', CT'', C', C_{i,1}', C_{i,2}')$.

5 Security Proof and Analysis

In this section we provide the security proof for our design CP-ABE scheme with the main security theorem, for CKA with search trapdoor in the standard model depends on Decisional Bilinear Diffie-Hellman (DBDH) and Decisional Linear (DLIN) assumption.

5.1 Decisional Bilinear Diffie-Hellman (DBDH) Assumption [14]

Defination5: Decisional Bilinear Diffie-Hellman assumption (DBDH)

Let $\mathbb{G}$, $\mathbb{G}_T$ be two multiplicative groups of a group $\mathbb{G}$ and e is bilinear pairing map. For the given elements $a,b,c,z \in \mathbb{Z}_p^*$ and $g, g^a, g^b, g^c \in \mathbb{G}$, $e(g,g)^{abc} = e(g,g)^R \in \mathbb{G}_T$ the DBDH assumption is defined as no probabilistic polynomial-time(PPT) adversary can decide the tuple $R = e(g,g)^{abc}$) or $e(g,g)^R$ with non-negligible advantage. An algorithm $\mathcal{A}$ that output $\tau \in (0,1)$ has advantages ϵ in solving the DBDH problem in $\mathbb{G}_T$.

Theorem1. The PPT adversaries has at most non-negligible advantages to broke our scheme in existing of DBDH and DLIN assumption, un-recoverable security against chosen keywords index and search token with non-negligible advantages $\frac{\varepsilon}{2}$.

Proof: Suppose there exists PPT adversary $\mathcal{A}$ who wants to break our scheme with none-negligible advantage ε. We build a challenger $\mathcal{C}$ which have the same non-negligible advantages ε in existing of DBDH and DLIN assumption. Challenger choose $a,b,c,z \in \mathbb{Z}_p$, $R \in \mathbb{G}_T$ let $R = abc$ the $\mathcal{C}$ give $(g, A, B, C, e(g,g)^{abc})$ from $(g, g^a, g^b, g^c, e(g,g)^z)$ query of $\mathcal{A}$ to return random bit $\tau \in (0,1)$. The answer to this challenge the challenger $\mathcal{C}$ play the security game as follow.

(Init) The adversary $\mathcal{A}$ submits two challenge access policy S_b^*=S_0^* , S_1^*, and access structure $\tilde{\mathrm{p}}_i^*$ of an unauthorized attribute's set A_i^*=$\{A_i^*\}_{i=1\ldots n}$ to the challenger $\mathcal{C}$ run the setup algorithm.

(Setup) The challenger $\mathcal{C}$ run setup algorithm for both CA(Setup), each attribute authority using bilinear map give g to an adversary. The adversary randomly choose $AA_i^* \subset AA_i$ for the corrupt authority $AuthN = AA_i - AA_i^*$ the reaming authority are non-corrupt the challenger sends public key of non-corrupt authority to $\mathcal{A}$. The $\mathcal{C}$ randomly choose $\alpha, \beta \in \mathbb{Z}_p^*$, $r_i, s_i \in \mathbb{Z}_p$ for the set of user's attribute's $(x_i, y_i) = e(g,g)^{-s_i\alpha\tilde{\mathrm{p}}_i r_i}$ compute public key and the master key kept secret as follow.

$\mathrm{PK} = (g, \mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{H}, \mathrm{R}, \{(\mathrm{x_i}, \mathrm{y_i})\}), PK_{Aid}, i \in [1, \mathrm{n}]$ and $M_{SK} = \{\alpha, \beta, R, \{r_i, s_i\}, i \in [1,n]$.

(Phase1) The challenger $\mathcal{C}$ generate an empty keywords set I_{wb} with the following adaptive queries.

(Outsource-Secret-Key-Query) The adversary query on outsourcing secret key of authorized attributes set and submit $A_i^* = \{A_i^*\}_{i=1\ldots n}$ a $sig(HGID^*, CA_{SK}u_{id}^*)$, a certificate the challenger first authenticate certificate with a public key of CA don't verify for A_i^*. If $\gamma(A_i^*, S) = 1$ the game is over with challenge access structure $\tilde{\mathrm{p}}_i^*$. Otherwise $\gamma(A_i^*, 1) = 0$ for the target access structure $\tilde{p}_i = (S, Attr_i \in \mathbb{A})$. The challenger compute $(x_i, y_i) = \prod_{i\in I} \tilde{p}.u_i, i \in [1,n]$,$y_i{}^w = \prod_{i\in I} e(g, g^{-\alpha r_i})^{w\tilde{\mathrm{p}}_i}$

and $x_i{}^w = \prod_{i\in I} e(g, g^{-\alpha r_i})^{w\tilde{\mathrm{p}}_i}$ assume $\tilde{\mathrm{p}} = g^{-\alpha}$ send the outsource secret key $e(g,g)^{\beta\tilde{\mathrm{p}}_i^*}$, the private key of challenge attribute set if adversary satisfies the target access structure. Since $A_i^* \not\subset \tilde{p}_i$ simply mean that $\mathcal{A}$ attributes set does not satisfy the access structure the challenger generate the secret key $SK_{idi}^* = HGID^* g^{(\alpha r_i)}$ for $\mathcal{A}$ and run the query search token algorithm.

(Token-Query) The $\mathcal{A}$ issue trapdoor queries for the keyword set $\{\tilde{\mathrm{w}}_{Lm}^*\} L \in [1,m]$. The challenger randomly choose $\sigma, \tau \in \mathbb{Z}_p$ generate a token for the $\mathcal{A}$ keywords set $w_{Lm'}^*$ as $TK_1 = Bg^{bH(w_\tau')}, TK_2 =$

$g^{\sigma\tau}$. An Adversary cannot satisfy the access policy for unauthorized attribute set $A_i^* \subset \tilde{p}_i$ the challenger add them to the keyword list $\widetilde{w}_{Lm}$ and send the tokens to the adversary.

(Challenge) Adversary generate keyword index $\widetilde{w}_{Lm}^* = g^{b(r_1+r_2)} g^{H(w_{\tau j})}$ select two random keywords set $\widetilde{w}_{0,Lm}^*, \widetilde{w}_{1,Lm}^*$ send to the challenger with $\widetilde{w}_{0,Lm}^*, \widetilde{w}_{1,Lm}^* \subseteq \widetilde{w}_{bLm}^*$. The challenger generates an empty keywords list I_{wb} for $\mathcal{A}$ does not exist in the $\widetilde{w}_{Lm} = g^{b(r_1+r_2)} g^{H(w_j{}')}$, $\widetilde{w}_{m'}$. The adversary again selects two keywords w_0 , w_1 that does not challenge before. The $\mathcal{C}$ run the keywords encrypts algorithm.

$\tilde{u} = g^{\theta} \prod_{j=1}^{m'} AU_i$ restraint $\mathcal{A}$ the challenge attribute set $A_i^* \in S$ cannot verify the access structure. The $\mathcal{A}$ need to distinguish g^{θ} from $g^{b(r_1+r_2)} g^{H(w_{\tau bj})}$ for $\widetilde{w}_{0,Lm}$ and $\widetilde{w}_{1,Lm}$ the $\mathcal{C}$ send keywords index set $|Index| = (\tilde{p}_i^*, I_{wb}\{\widetilde{w}_{Lm}, \widetilde{w}_m\}, L \in [1, m])$ to an adversary.

(Phase2) The adversary submits similar queries to phase1 at most q times with restriction no such keywords for the selected and legitimates keywords index can be existing. The probability to get g from R is same as the probability of $\tau = \tau'$. No such collision occurs in $\mathbb{G}$ and $\mathbb{G}_T$ in the general group model and hence the probability of collision is negligible.

(Gauss) The adversary makes a gauss at last $\tau' \in [0,1]$ where $\tau \neq \tau'$ the adversary consider $R = h^{r_1+r_2}$ is legitimate keywords search index the probability to solve the DBDH problem and recover $H(w_{bj}{}')$ form I_{wb} is negligible with non-negligible advantages of probability $\frac{\varepsilon}{2}$ as follow.

$=|\frac{1}{2}\Pr[\tau = \tau' \mid R = h^{r_1+r_2} = 0] + \frac{1}{2}\Pr[\tau = \tau' | R \neq h^{r_1+r_2} = 1] - \frac{1}{2}|$

$=|[\frac{1}{2} + (\frac{1}{2} + \varepsilon) - \frac{1}{2} \cdot \frac{1}{2}] - \frac{1}{2}| = \frac{\varepsilon}{2}$

Theorm2: Our proposed scheme un-revocable secure against cloud server, unauthorized user's attribute to provide privacy-preserving for data confidentiality, collision resistance in the system.

6 Correctness Verification of Keywords Search and Ciphertext Decryption

In this section, we provide the details of correctness analyses, the comparison of theoretical analysis, performance analysis, and complexity computation for our proposed CP-ABE scheme. This section consists of the correctness proof of successful keywords search and ciphertext decryption. We first analyze the correctness of matching keywords index with a search token the Eq. (1.3) verify.

$$Search(w_j') = e\left(\prod_{j=1}^{m'} (\widetilde{w}_{Lm}, TK_2\right) = e(I_w, TK_1) e(\widetilde{w}_{m'}, TK_3) \quad (1.3)$$

$= e(\prod_{j=1}^{m'} g^{c(r_1+r_2)} g^{H(w_j')}, g^{b\theta})$

$= e(g^{\theta}\ (\prod_{j=1}^{m'} (g^{bcr_1} g^{H(w_j')}) e(g^{bc\theta}, g^{r_2})$

$= e(g^{c(r_1+r_2)} g^{\sum_{j=1}^{m'} H(w_j')}, g^{b\theta})$

$= e(g,g)^{bc\theta(r_1+r_2)} e(g,g)^{b\theta \sum_{j=1}^{m'} H(w_j)})$

$= e(I_w, TK_1) e(\widetilde{w}_{m'}, TK_3)$

$= e\left(g^{\theta}, \prod_{j=1}^{m'} (g^{bcr_1} g^{bH(w_j')}\right) e\left(g^{bc\theta}, g^{r_2}\right)$

$= e(g^{\theta}, g^{bcr_1} \cdot g^{b\sum_{j=1}^{m'} H(w_j')}) e\left(g^{bc\theta}, g^{r_2}\right)$

$= e(g,g)^{b\theta \sum_{j=1}^{m'} H(w_j')} e(g,g))^{bc\theta r_1} e(g,g)^{bc\theta r_2}$

$= e(g,g)^{b\theta \sum_{j=1}^{m'} H(w_j')} e(g,g)^{bc\theta(r_1+r_2)}$

The decryption of ciphertext for authorized attribute's verify if, $\gamma(A_i, S) = 1$, $i \in S$ and $i \in [1, n]$ Eq. (1.5) as following.

$$Enk(CT_i) = \frac{msg(e(C\prod_{i\in I},C_{i,1},D_{(\pi)i,2})}{e(\prod_{i\in I} e(C_{i,2},D_{(\pi)i,1})} \tag{1.5}$$

$$=\frac{e(g,g)^{\alpha\beta\tilde{p}_i sr_i}\prod_{i\in I} e(u_i)^{s_i},g^{(\alpha u-\gamma_i)})}{\prod_{i\in I} e(x_i)^{s_i},g^{u-\beta-\gamma_i)}}$$

$$=\frac{e(g,g)^{\alpha\beta sr_i}\prod_{i\in I} e(g,g)^{-\tilde{p}_i s_i r_i \alpha u}\prod_{i\in I} e(g,g)^{\alpha\tilde{p}_i s_i r_i \gamma_i}}{\prod_{i\in I} e(g,g)^{-\alpha\tilde{p}_i s_i r_i u}\prod_{i\in I} e(g,g)^{\alpha\beta\tilde{p}_i s_i r_i}\prod_{i\in I} e(g,g)^{\alpha\tilde{p}_i s_i r_i \gamma_i}}$$

$$=\frac{e(g,g)^{\alpha\tilde{p}_i\beta sr_i}}{e(g,g)^{\alpha\beta\tilde{p}_i r_i\Sigma_{i\in I}\lambda_i\gamma_i}}$$

6.1 Performance and Theoretical Analysis Comparison

In this section, we provide a simulation result and the advantages of our scheme. In order to compare our scheme in terms of some characteristic efficiency, performance analysis, and complexity computation differences of our schemes in literature [14,16,17] are shown in Tab. 1 and Tab. 2. We used some variables for complexity computation representation where N is the least attributes that satisfy the access policy, n_i are the number of attributes in an initial access policy $n_{ri}{}'$ are the number of un-revoked users attribute's and $n_{ci}{}'$are the updated ciphertext under the new access policy. Where P is pairing operation, (E, m) is exponential and multiplication operation in the group $\mathbb{G}$, (E_T, m') are exponential and multiplication operation in a group $\mathbb{G}_T$. Similarly (L, j) are the encrypted and interested keywords search. Our CP-ABE the central authority authenticates both user's and AA_i in key generation verification to reduce security issues and support multi keywords search attribute revocation with policy updating. While Tab. 1 in [14] is tree-based that has lower efficiency and also does not support, multiple authority attribute revocation multi keywords search and policy updating and [17] is ABE does not support multiple authorities, attribute revocation, policy updating and similarly, we compare our scheme in Tab. 2 has an advantage over [16,17] while updating keys and ciphertext, to achieve an efficient user's attribute's revocation to generate a new attribute user's index set.

Table 1: Performances analysis comparison of our (CP-ABE) scheme

	Our Scheme	[14]	[17]
CP-ABE	Yes	Yes	NO
Multi-keywords-Search	Yes	No	Yes
LSSS-Structure	Yes	No	Yes
Revocation	Yes	No	No
Access-Policy	Yes	Yes	Yes
Policy-Updating	Yes	No	No
Security	CKA,TK	CPA	CPA,CKA
Multiple authorities	Yes	No	No

Table2: Comparison analysis computation complexity of our (CP-ABE) scheme

	Our-Scheme	[16]	[17]
Setup	$P + (n_i + 3)E + E_T$	$2P + (n_i + 2)E + E_T$	$(n_i + 4)E$
Key-Gen	$3P + (n_i + 7)E + 3m$	$(2n_i)E$	$(n_i + 6)P$
Encryption	$(n_i + j)E + 3m' + 2E_T$	$2(n_i + 2)E + (L + 2)P$	$(n_i + L + 6)E$
TK-Gen	$(L + 4)E + E_T + m'$	No	$(n_i + 4)E + 4P$
Search	$(j + 3)P + 2m$	$(2n_i + j)P$	$(j + 3)P$
Decryption	$(n_i + 3)E + 2m + (n_i + 3)E_T$	$2P$	$(P + 3)E$
Key-Update	$O(n_{ri}{}' + r)E + n_{ri}{}'P$	No	No
CT-Update	$O(n_{ci}{}')E + n_{ri}{}'P$	No	No

7 Conclusion

In this paper, we proposed a CP-ABE scheme to effective data access control for authorized attribute users with multiple authorities. The most critically the confidentiality of outsourcing data our access

control supports privacy preservation against collusion resistance. It also supports to achieves multi keywords search and the efficient user's attribute's revocation issue to related attribute authority through policy updating operation with minimal computational, communication load on data owner. Our scheme provides the details of security analysis of chosen keywords attack, search token, correctness verification and, performance analysis compare to the existing scheme. The security proofs related condition of our scheme for encrypted keywords index and search token are proven in a standard model using DBDH and DLIN assumption.

Acknowledgement: The work is partially supported by the Foundational Research Funds for the Central University (No. 30918012204). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which improved the presentation.

Funding Statement: This work is supported by the Foundational Research Funds for the Central University (No. 30918012204).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] 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 Transaction Parallel Distributed, Systems*, vol. 24, no. 1, pp. 131-143, 2013.

[2] R. Meng, Y. Zhou, J. Ning, K. Liang, J. Han and W. Susilo, "An efficient key-policy attribute-based searchable encryption in prime-order groups," *in 11th International Conference in Provable Security*, vol. 10592, pp. 39–56, 2017.

[3] J. Bethencourt, A. Sahai and B. Water, "Ciphertext policy attribute-based encryption," in *IEEE Symposium on Security and Privacy*, pp. 321-334, 2007.

[4] Y. Cheng, J. Ren, Z. Wang, S. Mei and J. Zhou, "Attributes union in CP-ABE algorithm for large universe cryptographic access control," *Second International Conference on Cloud and Green Computing*, pp. 180-186, 2012.

[5] Y. Miao, J. Ma, X. Liu, F. Wei, Z. Liu and X. A. Wang, "m^2-ABKS attribute-based encryption scheme multi-keyword search over personal health record in multi-owner setting," *Journal of Medical, System*, vol. 40, no. 246, 2016.

[6] Z. Liu, Z. Cao, Q. Huang, D. S. Wong and T. H. Yuen, "Fully secure multiple authority ciphertext policy attribute-based encryption without random oracle," *Computer, Security, ESORICS, Lecture Notes in Computer Science*, vol. 6879, pp. 278-297, 2011.

[7] H. Liu, P. Zhu, Z. Chen, P. Zhang, Z. L. Jiang, "Attribute-based encryption scheme supporting decryption and attribute revocation in cloud computing," *IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, 2017.

[8] W. Sun, S. Yu, W. Lou, T. Y. Hou and H**.** Li, "Protecting your right: verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in cloud computing," *IEEE Transaction Parallel Distributed, Systems*, vol. 27, no. 4, pp. 1187-1198, 2016.

[9] Q. Zheng, S. Xu and G. Ateniese, "VABKS: "Verifiable attribute-based keywords search over outsource encrypted data," *in IEEE Conference on Computer Communications*, pp. 522-530, 2014.

[10] J. Li, Y. Wang, Y. Zhang and J. Han, "Full verifiability for outsourced decryption in attribute-based encryption. *IEEE Transactions Services, Computing*, vol. 13, no. 3, pp. 478-487, 2017.

[11] S. Wang, K. Guo and Y. Zhang "Traceable ciphertext policy attribute-based encryption scheme with attribute level revocation for cloud storage," *PLoS One,* vol. 13, no. 9, 2018.

[12] H. Wang, X. Dong and Z. Cao, "Multi-value-independent ciphertext policy attribute-based encryption scheme with fast keyword search," *IEEE Transaction, Services, Computing*, pp. 1, 2017.

[13] S. Wang, J. Ye and Y. Zhang, "Searchable attribute-based encryption scheme with attribute update for cloud storage," *PLoS One*, vol. 13, no. 5, 2018. s

[14] H. Yin, J. Zhang, Y. Xiong, L. Ou, F. Li, S. Liao and K. Li, "CP-ABSE A ciphertext policy attribute-based searchable encryption scheme," *IEEE Access*, vol. 7, pp. 5682-5694, 2019.

[15] D. Li, J. Chen, J. Liu, Q. Wu and W. Liu, "Efficient CCA2 secure revocable multi-authority attribute-based encryption," *International, Symposium on Cyberspace, Safety and Security*, vol. 10581 pp. 103-118, 2017.

[16] J. Li, X. Lin, Y. Zhang and J. Han, "KSF-OABE: outsource attribute-based encryption scheme with keyword search function for cloud storage," *IEEE Transaction Services, Computing*, vol. 10, no. 5, pp, 715-725, 2017.

[17] S. Wang, S. Jia and Y. Zhang, "Verifiable and multi-keyword searchable attribute-based encryption scheme for cloud storage," *IEEE Access*, vol. 7, pp. 50136-50147, 2019.

[18] F. Guo, Y. Mu, W. Susilo, D. S. Wong and V. Varadharajan, "CP-ABE with constant-size keys for lightweight devices*," IEEE Transaction Information, Forensics and Security*, vol. 9, no. 5, pp. 763-771, 2014.

[19] Z. Liu, Z. L. Jiang, X. Wang and S. M. Yiu, "Practical attribute-based encryption: outsource decryption, attribute revocation and policy updating," *Journal of Network and Computer, Applications*, vol. 108, pp. 112-123, 2018.

[20] J. Li, W. Yao, J. Han, Y. Zhang and J. Shen, "Users avoidance CP-ABE with efficient attribute revocation for cloud storage," *IEEE System Journal*, vol. 12, no, 2, pp. 1767-1777, 2018.

[21] S. Agrawal and M. Chase, "FAME: "Fast attribute-based message encryption," *ACM, Conference on Computer and Communications*, pp. 665-682, 2017.