IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 15, Issue 5 Ser. I (sep – Oct 2019), PP 21-33
www.iosrjournals.org

A Verifiable Ciphertext Policy Attribute-Based Encryption(VCP-ABE) Scheme with Keywords Search and Revocation

Muqadar Ali,Chungen Xu, Abid Hussain, Laila Tul Badar
(Mathematics, Nanjing University of Science and Technology, China)
Corresponding Authors: Chungen Xu, Abid Hussain, Laila Tul Badar

Abstract:*Ciphertext policy attribute-based encryption(CP-ABE) scheme widely used in cloud storage for realizing the flexible and scalable fine-grained data access control for secure data sharing with user's under certain credential or attribute's. However most of the (CP-ABE) scheme have the problems such as access policy complexity, low computational efficiency, efficient revocation cannot be performed. Where traditional attribute-based encryption fails to provide efficient keyword's search due to week encryption scheme. In this paper we proposed verifiable ciphertext policy attribute based encryption(VCP-ABE) scheme with efficient attribute's user's revocation and secure keyword search on the encrypted keywords index using keywords search trapdoor where many of existing (CP-ABE) cannot support keyword search. The cloud server cannot learn any information about the keywordssearch trapdoor. Our proposed scheme achieves large universe set and multiple authority with flexible number of attribute's users. The data owner encrypts keywords index and ciphertext to cloud server under hidden access structure and access policy. Where many of outsource computing task can be done by the cloud proxy server CPS like outsource encryption, decryption and revoked related attribute's user's ciphertext update verification that greatly reduce the computational task at user's client side. We provide details of correctness analysis, performance analysis and security proof against chosen keywords attack in standard model for our scheme.*

Keywords:*Attribute-based encryption, Access control, Verifiability, Keyword search, Revocation*

Date of Submission: 27-08-2019 Date of Acceptance: 11-09-2019

I. Introduction

Attribute based encryption(ABE) is promising alternative technique that achieving fine grained access control for the encrypted data to related security threats via cryptographic mean. Where using public key encryption can be viewed as to share data with targeted users or the devices that should providing confidently from unauthorized users. The data provider knows the exact eligible user to share his data where the people are identified by the attribute's which is not realistic, in practical application for the data access control in which the data owner want to convey based on access policy for the privilege user's attributes. To solve this problem, the first attribute based encryption scheme ABE [1] proposed by Sahai and water where the attribute authority(AA) issues the secret key or key generation authority based on ABE for their attributes and the data provider specifies an access policy to set of attributes users. Only the users will be able to access and decrypt if he/she satisfy the access policy with access structure with associated ciphertext. To get a secret key each user's must prove the legality with set of attributes through set of trusted attribute authority. Goyal et al and Bethencourt [2,3] formalized two supplementary form of ABE ciphertext policy attribute based encryption(CP-ABE) and key policy attribute based encryption(KPABE). In (KP-ABE) [2] the ciphertext associated to attribute set and secret key attach to access policy for fine grained data access control for users to decrypted the ciphertext. The (CP-ABE) [3] the secret key attach to ciphertext and access policy connected to attribute set, where each users possess private key to corresponding attribute's set the ciphertext embedded into access policy, the attribute's users can be decrypt the ciphertext if his attributes satisfy the access policy. To overcome this problem of security and privacy the concept of multi authority AAs [4,5] was introduce with central authority and each authority distribute secret key correspond to the different set of attributes for the ciphertext decryption. Since in the presence of ABE solve the security issue but the users with different attributes user's access different level of encrypted data that fails the attribute user may be change with time that is imitated as attribute's revocation. To solve this problem with attribute user's revocation to periodically update key that allow only non-revoked user's to update secret key for thedecryption of newly encrypted data. In the scenario of revocable ABE [6] consists of two method i) indirect revocation in which the data sender encrypts his data under attribute set the and for fixed time the attribute authority according to revoked attribute list update the secret key for non-revoked attribute user's in each time periodically for the current ciphertext decryption. ii) Direct revocation in which sender during encryption algorithm specify the revocation list so that the data owner doesn't need to

update the secret key with instantly and without indirect revocation. Zheng et al [7] proposed Verifiable attribute-based keywords search (VABKS) searchable encryption scheme using access control policies for the keywords encryption. In the process of execution verification algorithm, the users whose credential satisfied the data owner access policy determined whether the sever return the verification algorithm for the desired policy and returned the information correctly. While the Scheme is less efficient due to access tree structure to related attribute and attribute revocation is not implement in his scheme. To achieve keywords based search and data access control several attribute based encryption has been proposed [8,9]. Which achieved keyword search encryption and data access control over the encrypted keywords index on using attribute based encryption technique his scheme also achieves attribute's user's revocation under with some limitation.

A. Related work

The efforts of scholar and researcher in cryptography achieve their own techniques in different field of cryptography for the purposes of data security. However, after the development of identity based encryption in cryptography that based on fuzzy identity encryption in [1] notion ofattribute-based encryption the attribute set represents identities the data sender need to specify some attributes for the data receiver no need of specify with specific identity where the attribute-based encryption has nice property that provide data access control the decryption side are not fixed. Then Ostrovsky et al in [10] proposed attribute-based encryption scheme of private keys for any access structure of Boolean formula that handle AND\OR gate including non-monotonic access structure one. After that Goyal et al [2] and Bethencourt [3] proposed for (KP-ABE) and (CP-ABE) based that based on attribute base encryption for the data access control access policy for security and privacy. Constant size ciphertext is also a type of ABE in research direction. Doshi et al [11] proposed fully secure constant size (CP-ABE) scheme to study about the access structure of attributes with secret key to an any subset of attribute can be part of ciphertext policy which creates the security issues for the proposed scheme. There are many multi authority attribute based encryption Yang et al [12,13,14] has been proposed for secure data access control that achieve the attribute revocation under random oracle model but these scheme cannot approach about the efficient access policy changes to new policy in attribute revocation for the encrypted data that provide forward security. Chen et al [15] presented a secure attribute based encryption scheme with threshold access structure for constant ciphertext in attribute based encryption and attribute based signature ABE/ABS. Further his design scheme support both KP-ABE and (CP-ABE) that applicable to large attribute universe with constant size ciphertext with ABS and reduce a pairing evaluation to a constant size, that has a nice property for practical attribute based encryption but his scheme cannot support keyword search and revocation. Qiu et al [16] formulized hidden ciphertext policy attribute based encryption keywords search scheme in which any user's only able to access and search the keywords if he\she satisfy the access policy of the data owner encrypted data and prove that his scheme secures under general group model for indistinguishable against keywords with access structure. Ciu et al [17] put a forward CP-ABE Scheme with partially hidden access policy with access structure give attribute's name, attribute's values are not given in the ciphertext where his scheme cannot support the attribute revocation and data verifiability that remains. After that Wang et al [18] presented a keyword searchable attribute based encryption and revocation scheme if the attribute set satisfy the access policy given token match to the keyword index the respective user's will be able to get the attach keywords query, but his scheme cannot clear about AND/OR gate access policy thus the scheme cannot achieve both AND/OR gate access policy only support AND gate access policy. To solve this problem, the Yin et al [19] proposed an efficient Ciphertext policy attribute-based searchable encryption scheme and support AND/OR gates access policy with threshold gates but his scheme the search token deterministic the query keywords in trapdoor vulnerable against chosen plain text attack. Lai et al [20] proposed verifiable ABE outsource decryption some extra information are added in ciphertext for the verification and transformation result correctness verification proof also his scheme support outsource decryption. Zhang et al [21] presented adaptively secure multi authority ABE that support outsource decryption verification but his scheme cannot support outsource encryption and verifiability. Wang et al [22] proposed Verifiable and multi keywords searchable attribute based encryption scheme for multi keywords the CS does not learn any information from keywords search trapdoor but his design scheme cannot support attribute revocation. Xiong et al [23] proposed a complicated Encryption Service Provider (ESP) verifiable scheme for outsource decryption result can be checked by the user's. Where they demonstrate that the intermediate ciphertext return to the user's by using either ESP scheme without any detection. In this paper we propose verifiable ciphertext policy attribute based encryption scheme keywords search and attribute revocation. Our VCP-ABE scheme consists secret key generation verification, outsource encryption, outsource decryption, and ciphertext update verification to ensure that ciphertext successfully update only non-revoked attribute users can access to new encrypted and updated data.

B. Contribution andChallenges

We proposed a verifiable ciphertext policy attribute-based encryption (VCP-ABE) scheme supporting attribute's revocation with keywords search in existing of central authority and multiple authority scenario that can be regarded with following contribution.

a) We proposed a (VCP-ABE) multiple authority scheme in the existing of central authority with keyword search and data access control for the authorized user's in order to support outsource encryption outsource decryption and ciphertext update verification through CPS that is high computing power to reduce workload on CS and user's client side.

b) In our Scheme each attribute authority first verifies the certificate of the user's for identification issued from central authority. If the user's is legal the corresponding attribute authority generate the secret key with unique identity of each user's that prevent the users from the collision attack.

c) We also design the attribute's revocation for multiple authority(AA_k) the central authority first completely remove the revoked user's from list with identity send the revoked user's list to attribute authority. The attribute's authority stop issuingto update key the list of revoked users with identity. The attribute authority periodically updates the secret key component for non-revoked attribute users to access and decrypt the new encrypt and update data on the basis of access policy verification.

d) In our proposed scheme the CS update the ciphertext after the secret key update while each attribute authority can verify the update ciphertext through CPS. The CPS return 1 mean the ciphertext successfully updated otherwise output 0 in case of unrevoked attribute's user's.

e) In order to resolve the issue of collision all users in the system to prevent collision attack it is necessary for the compromising security. The revoked user's cannot able to combine their secret key information with revoke identity of non-revoked attribute's users with unique identity verification from the attribute authority in key updating process. Hence the revoked attribute users cannot use the old keys to update his secret key and decrypt newly created ciphertext.

The reminder of this paper is organized as follow.

In section II we briefly review preliminaries and some definition associated with this work. System model, system framework and security model in section III. The scheme concreates construction of (VCP-ABE) scheme including revocation system security and correctness analysis explain in section IV. In section V we compare our scheme previous existing scheme and then extend our (VCP-ABE) with keyword's search and multiple authority revocability scheme with improve efficiency. Finally, we conclude this paper in section VI.

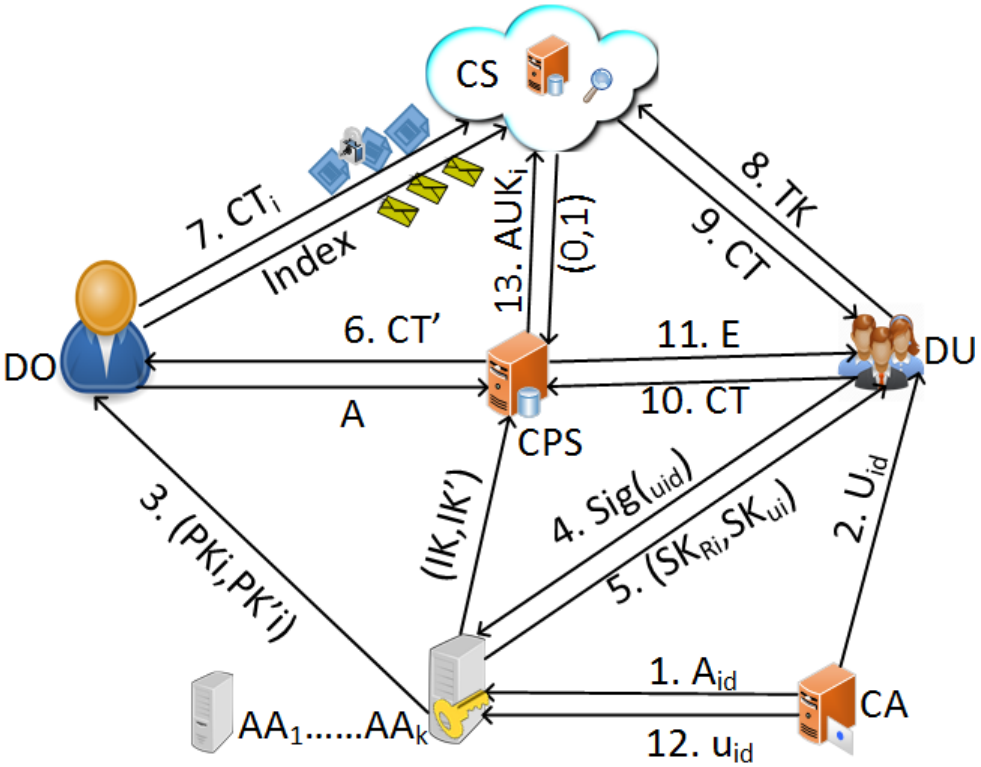

Figure1 System Model

II. Preliminaries

In this section we review some of the basic cryptographic definitions including Bilinear maps, Access structure and Linear secret sharing scheme that are related to our verifiable ciphertext policy attribute-based encryption scheme.

A. Deination1: Bilinear maps

Let $\mathbb{G}_1, \mathbb{G}_2$ be two multiplicative cyclic group of prime order $p$where g is generator of group $\mathbb{G}_1$. A bilinear pairing constructed with following properties.

1)Bi-linearity For all $u, v \in \mathbb{G}_1$and $x, y \in \mathbb{Z}_p^*, e(u^x, v^y) = e(u, v)^{xy}$ exists.

2)Non-degeneracy $e(g, g) \neq 1$, where g is generator of group $\mathbb{G}_1$

3)Computability For all $u, v \in \mathbb{G}_1$ there exist an efficient polynomial time algorithm $e(u, v) \in \mathbb{G}_2$.

B. Deination2: Access Structure [24]

Let $\mathbb{L} = \{L_1, L_2, \dots L_k\}$ be set of attributes a collection $\mathbb{A} \subseteq 2^{\{L_1, L_2, \dots L_k\}}$ if $\forall B, C$: if $B \in \mathbb{A}$ and $B \subseteq C$ then $C \subseteq \mathbb{A}$ an access structure respectively, monotonic access structure and monotonic access structure is a collection respectively, monotonic collection of $\mathbb{A}$ non-empty subset of $\mathbb{L} = \{L_1, L_2, \dots L_k\}$i.e$\mathbb{A} \subseteq 2^{\{L_1, L_2, \dots L_k\}} \setminus \{\emptyset\}$. Thus the set in $\mathbb{A}$ is called authorized attributes sets and the sets not in $\mathbb{A}$ is called non-authorized attributes sets.

C. Defination3: Linear secret sharing scheme [25]

A linear secret sharing scheme is set of attributes $\mathbb{L}$ of matrix M with l row and n column. Let ρ be a function as $\rho: 1, \dots, l \to \mathbb{L}$ that map each row of M to an attributes set for labeling. A secret sharing scheme Π is set of attributes $\mathbb{L}$ is called a linear secret sharing scheme over $\mathbb{Z}_p$ if,

1) The share for each attribute from a vector over $\mathbb{Z}_p$.

2) There exist a matrix M with l row and n column called the sharing generating matrix for Π. For $i = 1, \dots, l$ we let the function ρ is map each attributes of matrix to an attributes i is $\rho(i)$. Considering that column vector v=(s,r_1,…,r_n) and s∈ $\mathbb{Z}_P$ is share of secret to be shared and r_1,…,$r_n \in \mathbb{Z}_p$are randomly chosen then $M(v)i$ is called l share according to Π and share $M(v)i$ belong to attribute $\rho(i)$. According to linear reconstruction property of Π is LSSS for access structure $\mathbb{A}$ and $L_i \in \mathbb{A}$ be authorized set of attributes and $I \subset \{1, \dots, l\}$ can be define as $I = \{i: \rho(i) \in L_i\}$. Then the vector $(1,0, \dots ,0)$ is in the span of row of matrix M indexed I there exist a constant $\{\omega_i \in \mathbb{Z}_P\}$ such that if γ_i is valid share s according to Π, then $s = \sum_{i \in I} \omega_i \gamma_i$ for authorized set otherwise for unauthorized set no such constant are existing.

Boolean Formula. LSSS access structure can be derived from representation of Boolean formulas. There are generic methods to convert monotonic Boolean formula into LSSS matrix. A Boolean formula can be represented as an access tree in which AND/OR gates denote an interior nodes and attribute are denoted in leaf nodes. The number of leaf nodes in the access tree are equal to the number of rows in LSSS matrix.

Table1 Notations used in this Paper

Notation	Description
PK_{CA}	Public key of central authority
$\mathbb{L}$	Least number of attributes satisfy access policy
L_i	The number of attributes satisfy access policy
A_{id}	All attribute authority identity
SK_{Aid}	Authority secret key
Uid	All user's identity
uid	Each user's identity
SK_{uid}	Certificate holder user's secret key
AA_k	Number of attribute authority
$Sig(uid)$	Certificate signature
$\mathbb{A}$	Access structure
$\mathcal{S}$	Access policy
SK_{ui}	User's secret key
RK_i	Attribute user's Retrieval key
IK_i	Intermediate key
TK_i	User's keywords search token
CT_i	Encrypted ciphertext
CT'	Re-encrypted ciphertext
E	Outsource decrypted ciphertext

III. System Model And Security Model

In this section we present system model and security model for our verifiable ciphertext policy attribute-based encryption keywords scheme(VCPABE) that consists six entities to performed efficient, verifiable and flexible multi keywords search on outsource encrypted data.

A. System model

As shown in Fig1 the system model for (VCPABE) verifiable ciphertext policy attribute-based encryption keywords search under the scenario of cloud storage consists of six entities the Central authority(CA), Attribute authorities Data owner (DO), Data users(DU), Cloud server(CS) and Cloud proxy Server(CPS).

1)Central authority: Central authority is fully trusted authority that is responsible for the System initialization registration for both attribute authority and users it's also provide certificate to legal user's and send revoked user's list at revocation time that is that required for the system security. Where Central authority does not participate any attribute related operation.

2) Attribute Authority: The Attribute authority is trusted authority that responsible for verification of user's certificate to generate secret key for attribute user's and the distribution of secret key according to ownership of legal user's identity, or role based access control and public key under a secure way. The attribute authority also responsible secret key update in revocation time for non-revoked attribute's user's.

3)Data Owner: The data owner first defines access control, access structure and access policy for the attribute user's in the system the data he intends to outsource to the cloud server. The data owner run keyword index generation algorithm to generate keywords index and ciphertext then extract index keywords from data file to corresponding attribute's set that involve in the access policy for the define access structure. For the better data confidentiality, the data owner uses symmetric encryption key like AES symmetrically encrypt the keywords index and ciphertext to cloud server. Only the attributes users can search and decrypt the ciphertext if he\she satisfy the access structure embedded in ciphertext.

4)Cloud server(CS) Cloud server has the capacity to store a large amount of date it provides data storage service for the data owner to encrypt all the data that consist of keywords search index with corresponding ciphertext. Further its provide search facilities for the user's in based on query interested keywords search token. The CS return the search result to the user's if search token match to the interested keywords index successfully output 1 otherwise 0 while the server has no knowledge about the index keywords and trapdoor keywords search query. Further the CS update all the ciphertext after the updating of secret key related to revoke attribute's users.

5)UsersThe user's is authorized set where each user's has unique identity uid, certificate that labeled with attribute's. The user's request to generate secret key from the related attribute authority and search token generated by CS for query keyword search. All users can freely download the ciphertext and decrypted the encrypted data with their secret key if he/she satisfy the access structure for and access policy.

6)Cloud Proxy Server (CPS) The Cloud proxy server has powerful computing ability to helps data owner, user's and attribute authorities in outsource encryption, outsource decryption, and updated ciphertext verification to ensure an efficiency in attribute revocation that reduce the computational workload on user's client where the cloud proxy server is also semi trusted that get no information about the ciphertext.

B. Access Control frame work

To fulfil the requirement of verifiable Ciphertext policy attribute-based encryption scheme with keywords search including central authority, attribute authorities, data owner, multi user's, Cloud sever and Cloud Proxy server our (VCP-ABE) scheme consist of fifteen algorithms as follow.

1)CA Setup$(\kappa) \rightarrow (PK_{CA}, SP)$ The central authority(CA) execute the algorithm input security parameter κ and output central authority public key and system parameter.

2)AA Registration $(A_{id}, SP) \rightarrow (PK_{aid}, SK_{Aid})$The CA assign each attribute authority(AA_k) with authority identity A_{id} for all legal attribute's authority output authority public key and each authority secret key.

3)Users Registration$(SP, PK_{CA}) \rightarrow (SK_{uid}, Uid, Sig(uid))$This algorithm is run by the Central authority that input system parameter central authority pubic key, and output secret key with certificate for all legality users with corresponding certificate.

4)AA Setup(PK_{aid}, L_i) $\rightarrow$ (PK_{Li}, MK) Each attribute authority(AA_k) input its public key issue from central authority, attribute's set L_i that managed by each authority output public keys of attribute's user's and master key.
5)Key-Gen($PK_{aid}, L_i, Uid, Sig(uid), SK_{uid}$) $\rightarrow$ (SK_{ui}, RK_i, IK_i)Each attribute authority(AA_k) run secret key generation algorithm input authority public key, attribute's user's set, all users identity certificate with secret key output secret key for all user's and intermediate key and retrieval keys RK_i for the attribute's user's.
6)Index generation($PK_{aid}, W_D, W_D^{'}$) $\rightarrow$ ($|Index|$)The data owner run the keywords index generation algorithm that input authority public key keywords set and interested keywords and output Keywords index.
7)Encrypt($PK_{aid}, \mathbb{A}, \mathcal{S}, |Index|$) $\rightarrow$ (CT_i) The DO run the encryption algorithm input attribute authority public key, access structure $\mathbb{A}$, access policy $\mathcal{S}$ and output the ciphertexts CT_i while the encryption algorithm consists of outsource encryption and encryption of ciphertext, and keywords index.
8)Gen-TK($PK_{aid}, \mathcal{S}, SK_{ui}$) $\rightarrow$ (TK_i) The token generation algorithm run by attribute's user's to generate token for query keywords that input the authority public key, access policy and its secret key output the search token for all legal user's.
9)Search($TK_i, W_D^{'}$) $\rightarrow$ ($1, \perp$) The CS execute the search algorithm token submitted by the user's the CS verifies that search token match to encrypted interested keywords of the attribute's user's , if verification is successful the CS send the query keywords search result otherwise $\perp$.
10)Decrypt($\mathbb{A}, RK_i, CT_i$) $\rightarrow$ ((msg), $\perp$) This algorithm run by the user's input access structure retrieval key for the decryption of ciphertext the decryption algorithm consists of outsource decryption that is run by the CPS and decryption algorithm run by the CS. The CS successfully output the $Enk(msg)$ if he\she satisfied the access structure embedded in ciphertext otherwise $\perp$.
11)Revocation(PK_{aid}, LR_i, uid) $\rightarrow$ ($LR_i^{'}$) The attribute revocation algorithm is run by each attribute authority input the authority public key, previous attribute's list and each revoked user's identity list issue by the CA output new non-revoke attribute's user's list. Where the central authority removes the certificate with unique identity of revoked user's send the list of revoked user's to attribute authority.
12)Authority-Key-Update($PK_{aid}, LR_i, MK, SK_{Aid}$) $\rightarrow$ ($PK_{aid}^{'}, MK^{'}, SK_{Aid}^{'}$) This algorithm run by each attribute authority(AA_k) input previous attribute authority public key master secret key, attribute's users revocation list output each attribute authority updated public key, master key and secret key.
13)Users-Key-Update($PK_{aid}^{'}, MK^{'}, u^{'}id, SK_{ui}$) $\rightarrow$ ($SK_{ui}^{'}, RK_i^{'}, IK_i^{'}$)) The attribute authority(AA_k) run user's keys update algorithm that input authority updated public key, master key non revoked user's identity attribute user's current key output update secret keys retrieval keys and intermediate key for all non-revoked attribute's user's.
14)CT-Update($CT_i, AUK_i, PK_{aid}^{'}, MK^{'}$) $\rightarrow$ ($CT_i^{'}$) The ciphertext update algorithm run by the cloud server input current ciphertext and attribute's user's updated keys and output the update ciphertext for unrevoked attribute user's.
15)Verify($AUK_i, LR_i^{'}$) $\rightarrow$ (1,0) The attribute authority(AA_k) run the ciphertext update verification algorithm input attribute's user's update keys, non-revoked attribute's user's list request from CPS the correctness verification of update ciphertext the CPS output 1 ciphertext $CT_i^{'}$ successfully updated if the verification is successful otherwise 0.

C. Security Model

The security of our proposed revocable Verifiable ciphertext policy attribute-based encryption with keywords search of our scheme based on Decisional Bilinear Diffie Hellman assumption and Decisional linear assumption where the CS cannot collide with revoked attribute user's but sever also curious that perform the operation for encrypted data. For our scheme we define security model under central authority non adaptive security game procedure between the adversary $\mathcal{A}$ and the challenger $\mathcal{C}$ and adversary set the authorities as corrupt authoritiesto get the system parameter send the entire query to the challenger $\mathcal{C}$ as follow.
(Adversary queries) The adversary $\mathcal{A}$ choose a random bit $b^{'} \in (0,1)$ and send entire query to the challenger where challenger $\mathcal{C}$ run CA setup algorithm and reply the adversary $\mathcal{A}$ queries.
CA Setup(κ) $\rightarrow$ (PK_{CA}, SP) The challenger $\mathcal{C}$ run the CA setup algorithm for the set of corrupt authority and output public key and system parameterSP for corrupt authority of adversary $\mathcal{A}$ with following queries.
a)(Public-Key-Query) The adversary $\mathcal{A}$ makes query for authority public key(APK_{aid}) for all corrupt authority AA_C^* as APK_{aid}^* by himself and send to the challenger $\mathcal{C}$. Where the challenger $\mathcal{C}$ run the setup algorithm sends the public key to adversary $\mathcal{A}$ and keep master key secret.
b) Secret-Key-Query$\left(APK_{aid}^*, L_i^*, U_{id}^*, Sig(u_{id}^*)\right)$ $\rightarrow$ ($SK_{ui}^*, RK_i^*, IK_i^*$) The adversary $\mathcal{A}$ query for the secret key submit challenge unauthorized attribute's, user's identity and certificate that is not issue from the central authority the challenger $\mathcal{C}$ run the key generation algorithm challenger $\mathcal{C}$ first compute and verify the certificate and authenticate that U_{id}^* is the identity for all user's adversary which not in the list of central authority because

$u_{id}^{*} \neq u_{id}$ for legal and register user's where L_i^* attribute set issue from corrupt authorities and does not satisfied the target access structure $\mathbb{A}$ for the attribute's user's $L_i^*, i \in [1,k]$. For the corrupt (AA_C^*)authorities the challenger $\mathcal{C}$ run the key generation algorithm and send corresponding secret key $SK_{uid}^{*}\{u_{id}^{*} \neq u_{id}\}, RK_i^*, IK_i^*$to the adversary $\mathcal{A}$.

c)Token-Query The adversary $\mathcal{A}$ choose interested keyword $W_D^{''}$ with challenge access structure $\mathbb{A}^*$, SK_{uid}^{*} and access policy $\mathcal{S}^*$submit to the challenger $\mathcal{C}$ that does not satisfy the challenge access structure, access policy. The challenger $\mathcal{C}$ run the token generation algorithm on the basis of secret key algorithm $SK_{uid}^{*}\{u_{id}^{*} \neq u_{id}\}$ and send token to the adversary $\mathcal{A}$ that does not match the legitimate interested keywords$W_D^{'}$.

d)Keyword-Query The adversary $\mathcal{A}$ choose keywords set W_D^* and send to the challenger $\mathcal{C}$ the limitation is that the adversary $\mathcal{A}$ satisfy the access structure $\mathbb{A}^*$ for chosen keywords W_D^* than challenger create empty keywords set W_D access structure $\mathbb{A}$, access policy $\mathcal{S}$ for attribute's user's and run the keywords encrypt algorithm the restriction is that for W_D^* the adversary $\mathcal{A}$ cannot satisfy the access structure and access policy that perform as corrupt the adversary $\mathcal{A}$ chose corrupt authorities and cannot match to the legitimate keywords set W_D.
(Guess). The advantage of the Adversary $\mathcal{A}$ in above game output b_0 of $b^{'}$ with probability.
Prob $[\mathcal{A}(|b_0{=}b^{'}|) - \frac{\varepsilon}{2})]$.

IV. A Verifiable Ciphertext Policy Attribute-Based Encryption With Keyword's Search And Attribute's Revocation

In this section the concreate construction of our proposed Verifiable Ciphertext policy attribute-based encryption with keywords search for outsource encrypted data and attribute's user's revocation for each algorithm are as follow.

A. System Setup

1) CA Setup$(\kappa) \rightarrow (PK_{CA}, MK, SP)$ The central authority no input other than security parameter κ output central authority public key, master key and system parameter choose a bilinear maps of prime order p and generator g of a group $\mathbb{G}_1$with hash function $\mathbb{H}(0,1)\rightarrow \mathbb{Z}_P^*$, e:$\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ First compute
$SP = (e, \mathbb{G}_1, \mathbb{G}_2, Uid, AA_K, g, \mathbb{H})$ choose $a \in \mathbb{Z}_P^*$ generate $PK_{CA} = g^a$ public key and master key.
2)Users-Registration$(SP, PK_{CA}, MK) \rightarrow (SK_{uid}, Uid, Sig(Huid))$ The CA input system parameter, public key and master key and output secret key for each legal user, all users with unique identity and certificate for all users join in the system. Randomly choose $u_i, r_i \in \mathbb{Z}_P$ compute $SK_{uid} = g^{H_1(u_i r_i)}$ where Uid is the universe set of user's with unique identity and certificate $Sig(uid)) = (H(uid)g^{H_1(u_i r_i)})$.
3)AA-Registration $(A_{id}, SP)) \rightarrow (PK_{aid}, SK_{Aid})$ The CA input each authority identity, system parameter output the authority public key PK_{aid} and secret key. The CA assign each authority with A_{id} with system parameter SP if and only if the authority is legal.
4)AA-Setup$(PK_{aid}, L_i) \rightarrow (PK_{Li}, MK)$ Each attribute authority(AA_k) input its public key issue from central authority, attribute's set L_i that managed by every authority output public key, master key of attribute authority with A_{id} the authority must be register from CA. Randomly choose $\alpha, \sigma \in \mathbb{G}_1$ and set $PK_{aid} = g^{\sigma}$ where
$X = \prod_{i=1}^{k}(L_i, u_i)$,$PK_i$ =$(g, \mathbb{G}_1, e, \mathbb{G}_2, X, \mathbb{H}, \{PK_{Li}\}, 1 \leq i \leq k]$ and $MK = (\alpha, \sigma), g^{\alpha}, 1 \leq i \leq k)$ and where each attribute's connected to some user's $U = \{u_1, u_2, \dots, u_k\} = \{L_1, L_2, \dots, L_k\}$ indicate number of attribute's with their respective user's.
5)Key-Gen$(PK_{aid}, MK, L_i, Uid, Sig(H(uid)) \rightarrow (SK_{ui}, RK_i, IK_i)$ Each attribute authority(AA_k) input public key master key attribute's user's set, all users identity and certificate and output secret keys, retrieval keys and intermediate keys for all user's. The users can request for the secret key with certificate the authority verify the certificate $Sig(uid)) = verfy(H(uid)^{u_i} g^{\pi}, PK_{CA})$ authority first calculate $\pi = u_i H_1(r_i)$ and $\varphi = Sig(uid)^{u_i}$ where π and φ are the verification function for attribute's users secret key generation.
$=e(\varphi, g) = e(SigH(uid).g^{\pi})^{u_i}, PK_{CA})$…….(1)
$= e(SigH(uid)^{u_i}.g^{H_1(u_i r_i)}, g^{a})$
$= e(SigH(uid)^{u_i}.g^{\pi}, g^{a})$
$= e(SigH(uid)^{u_i}.SK_{uid}, PK_{CA})$

The certificate verification is using for the purposes of identification if user's legal then(AA_k) generate secret key and corresponding retrieval keys and intermediate key where $IK = (U_i, L_i, \mathbb{A}), i \in [1,k]$. Then for authorized attribute's users with Uid and $Sig(uid)$ generate the content key as randomly take $x, r_i, s_i \in \mathbb{Z}_P \alpha, u \in \mathbb{G}_1$compute$D_{i,1} = g^{(u-\omega_i)} D_{i,2} = g^{\gamma_i + \alpha s_i}$ while output SK_{ui} if $L_{ui} \in \mathbb{A}, i \in [1,k]$ satisfy the access structure and generate and RK_i is retrieval key for the outsource decryption. Output $SK_{ui} = \left(D_{i,1}, D_{i,2}\right), i \in SRK_i = g^{xr_1\alpha}$.

6)Index-Gen($PK_{aid}, W_D, W_D^{'}$) $\rightarrow$ ($Index$)The data owner input authority public key keywords set and interested keywords randomly choose $a, c, t, r_i \in \mathbb{Z}_P \alpha \in \mathbb{G}$and compute Keywords index $W_D = g^{t(r_1+r_2)} g^{H\left(W_j^{'}\right)}$and $W_D^{'} = g^{ac\alpha} \in \mathbb{G}_1, j \in [1, m]$,$W_D (1 \leq j \leq m)$ output Keyword index $W_D$and $W_D^{'}$.

7)Encryption:
a)Outsource-Encryption($PK, CT, \mathcal{S}$) $\rightarrow$ ($CT^{'}$)The CSP input attribute's users public key, ciphertext and access policy $\mathcal{S} = (M, \rho)$ where M is matrix of $l \times n$ and ρ is for attribute's that map each row of matrix M to an attribute's set output re-encrypted ciphertext $CT^{'}$ compute$CT^{'} = (\mathcal{S}, \{C_1, C_{i,1}, C_{i,2}, PK(CT)\rho_i\}, i \in [1, l]$.
b)Encrypt($PK_{aid}, \mathbb{A}, \mathcal{S}, W_D, W_D^{'}$) $\rightarrow$ ($CT_i, |Index|$) The DO input attribute authority public key, access structure $\mathbb{A}$ access policy $\mathcal{S}$ keywords set, interested keywords output the ciphertext$CT_i$and keywords index. The access policy $S = (M, \rho)$ where the ρ is a map each M_i of matrix M to an attributes (ρi) randomly choose $x, s_i, r_i \in \mathbb{Z}_{\mathrm{P}}, \alpha, u \in \mathbb{G}_1$ and two random vector as $\upsilon = (s, \upsilon_1, \upsilon_2, \dots, \upsilon_n)^T$ and $y = (0, \eta_1, \eta_2, \dots, \eta_n)^T$for $i = 1\ to\ l$ its compute $\omega_i = M_i \upsilon$ and $\gamma_i = M_i \eta$ then $X = \prod_{i=1}^{k} (L_i, u_i) \dots\dots\dots (2)$ where X denote the each attribute's that assign to specific user's its randomly choose $r_i, s_i \in \mathbb{Z}_{\mathrm{P}}$ compute $CT = m.e(g, g)^{x\alpha s_i r_1}$ $CT^{'} = g^{si}, C_1 = e(g, g)^{r_1 s}$, $C_{i,1} = g^{-\alpha s_i r_1}$ and $C_{i,2} = g^{r_1 \omega_i}$ output the ciphertext $CT_i = (\mathbb{A}, CT^{'}, C_1, C_{i,1}, C_{i,2})$ data owner finally upload the keywords index and ciphertext symmetrically to cloud server $\left(\mathbb{A}, |Index|, CT, CT^{'}, C_1, C_{i,1}, C_{i,2}\right)$.

8)Gen-TK($PK_{aid}, \mathcal{S}, SK_{ui}$) $\rightarrow$ (TK_i) The attribute's user's input authority public key, access policy and its own secret key output the token for all legal user's the sever return token the attribute user's if $i \in \mathcal{S}, i \in [1, k]$ return token to authorized user's randomly choose $a, t, r_i \in \mathbb{Z}_{\mathrm{P}}, \alpha \in \mathbb{G}_1$, $TK_{i,1} = g^{\frac{ac\alpha}{t}}$, $TK_{i,2} = g^{r_1+r_2} \cdot \prod_{j=1}^{D^{'}} g^{\frac{H(W_j^{'})}{t}}$

9)Search($TK, W_D^{'}$) $\rightarrow$ ($1, \perp$) The CS execute the search algorithm token submitted by the user's the CS verifies that search token match to encrypted interested keywords of the attribute's user's, if verification is successful the CS send the query keywords search result and output 1 otherwise $\perp$.
Judge($W_j^{'}$)= $e\left(\prod_{j=1}^{D^{'}} (W_D, TK_{i,1}\right) = e\left(\mathrm{W}_{D^{'}}, TK_{i,2}\right)$……(3).
If users satisfy the access structure for search query keywords the CS judge whether the token submit from user's side match to $TK_{wq} = w_i$ equation3 true or not. The data owner encryptskeywords index as $X = \prod_{i=1}^{k} (L_i, u_i), i \in [i, k]$for attribute's user's whose want to search and generate a token in interested keywords must satisfy the above equation. The CS match the token to interested keywords if search token match the CS successfully return the search result attribute user's$L_{ui} \in \mathbb{A}(W_D^{'}(j = q = 1)$if attribute user's $L_{ui} \notin \mathbb{A}(W_D^{'}(j = q = \perp\}$otherwise output$\perp$ in such condition the user's not allow to search on query keywords.

10)Decryption
a)Outsource decryption($PK, IK_i, CT^{'}$) $\rightarrow$ (E) The CSP input public key intermediate key and re-encrypted ciphertext output the partial decrypted ciphertext. If $Luid \notin \mathbb{A}$ the algorithm output an error message otherwise its compute $I = \{i: \rho(i) \in L_i\}, i \in [1, l]$ with constant $\omega_i \in \mathbb{Z}_P$ such that $\sum_{i \in I} \gamma_i \omega_i = (1, 0, \dots, 0)$and output the partial decrypted ciphertext E outsource decryption operational algorithm and send to user's as.
$(E) = \frac{e(C_1 \prod_{i \in I} (C_{i,1}, D_{i,1})}{e(\prod_{i \in I} e(C_{i,2}, D_{i,2})}$……. (4)

b)Decryption(RK_i, CT_i) $\rightarrow$ ($(msg), \perp$) The user's input its retrieval key for the decryption of ciphertext. The attribute user's successfully output the message satisfy the access structure embedded in ciphertext otherwise if $Luid \notin \mathbb{A}$ output $\perp$.According to LSSS property if γ_i are valid share for secret s there exist such constant $\{\gamma_i \in \mathbb{Z}_P\}, i \in I$ such that $s = \sum_{i \in I} \gamma_i \omega_i$the user's compute $RK_i$and decrypt file with retrieval key as follow.

$$msg = \frac{CT.e(C_{i,1}, g)^{u+x}}{E} \dots\dots (5)$$

11)Revocation(PK_{aid}, LR_i, uid) $\rightarrow$ ($LR_i^{'}$)Each attribute authority(AA_k) input the authority public key, revoked attribute's list and each user's identity output newnon-revoke attribute's list. Where the central authority removes the certificate and identity of revoked user's send the list of revoked user's to attribute authority. The attribute authority generate new attribute list that is $LR_i^{'}$ for non-revoked user's. The revocation of attribute users contains two algorithms a) Key-Update b) Ciphertext-Update to ensure that revoked attribute cannot decrypt the data while the new users can decrypt the previous data if his attribute satisfy the access policy.

12)Authority-Key-Update($PK_{aid}, LR_i, MK, SK_{Aid}$) $\rightarrow$ ($PK_{aid}^{'}, MK^{'}, SK_{Aid}^{'}$) Each attribute authority(AA_k) input previous attribute authority public key, master key, attribute's users revocation list output each attribute authority updated public key, master key and secret key. Randomly choose $\alpha^{'}, \sigma^{'} \in \mathbb{G}_1$ and set $X = g^{\alpha^{'}}$ where $X^{'} = \prod_{i=1}^{k}(LR_i^{'}, u_i{'})$ is non-revoked attribute's user's in revocation phase
$PK^{'}$ =(g,$\mathbb{G}_1$, e, $\mathbb{G}_2$, X, $\mathbb{H}$,{$PK_{Li}^{'}$},$1 \le i \le k$] and $MK^{'} = (\alpha^{'}, \sigma^{'}), g^{\alpha^{'}}, 1 \le i \le k$).

13)Users-Key-Update($PK_{aid}^{'}, MK^{'}$) $\rightarrow$ ($SK_{ui}^{'}, RK_i^{'}, IK_i^{'}$) The attribute authority AA_k input authority updated public, master key output the update secret keys, intermediate key and retrieval keys for all non-revoked attribute's user's. Then for non-revoke attribute's user's with Uid and $Sig(uid)$ update the key as randomly choose $u^{'}, \alpha^{'} \in \mathbb{G}_1, x^{'}, s_i^{'}, r_i^{'} \in \mathbb{Z}_P$ compute$D_{i,1} = g^{(u^{'}-\omega_i^{'})}, D_{i,2} = g^{(\gamma_i^{'}-\alpha^{'}s_i)}$ while output $SK_{uid}^{'}$ if
$LR_i^{'} \in \mathbb{A}, i \in [1,k]$ satisfy the access structure output $SK_{uid}^{'} = \left(D_{i,1}, D_{i,2}\right)$and
$RK_i^{'} = g^{x^{'}\alpha^{'}r_1^{'}} IK_i^{'} = \{U_i^{'}, LR_i^{'}, \mathbb{A}\}$. The revoked user's cannot use non-revoked user's secret key to update its own secret key hence $SK_{uid} \neq SK_{uid}^{'}$.

14)CT-Update($CT_i, AUK_i, PK_{aid}^{'}, MK^{'}$) $\rightarrow$ ($CT_i^{'}$) The ciphertext update algorithm run by the cloud server input current ciphertext and attribute's user's updated keys. Output the current updatedciphertext for the unrevoked attribute user's randomly choose $x^{'}, r_i^{'}, s_i^{'} \in \mathbb{Z}_P$ update each ciphertext to related attributes' user's as follow.
$CT^{'} = e(g,g)^{x^{'}\alpha^{'}s_i^{'}r_1^{'}}, CT^{''} = g^{s_i} = CT^{''} = g^{s_i^{'}}, C_1 = e(g,g)^{r_1 s} = C_1^{'} = e(g,g)^{r_1^{'}s^{'}}, C_{i,1} = g^{-\alpha s_i^{'} r_1}, C_{i,1}^{'} = g^{-\alpha^{'}s_i^{'}r_1^{'}}$ and $C_{i,2} = g^{r_1\omega_i} = C_{i,2}^{'} = g^{r_1^{'}\omega_i^{'}}$ output the update ciphertext $CT_i^{'} = (\mathbb{A}^{'}, CT^{'}, CT^{''}, C_1^{'}, C_{i,1}^{'}, C_{i,2}^{'})$.

15)Verify($AUK_i, LR_i^{'}$) $\rightarrow$ (0,1) After the ciphertext update the attribute authority(AA_k) input attribute's user's update keys, non-revoked attribute's user's list and request from CPS the correctness verification of update ciphertext. The CPS output 1 if the ciphertext update correctly otherwise 0. For the correctness and access to updated ciphertext the following condition must hold.
a)($AUK_i, CT_i^{'}, LR_i^{'}$) $\rightarrow$ (m, 0) If $u_{id}^{'} \in LR_i^{'}$ the non-revoked user's whose satisfy the access structure with corresponding update secret key output m where $u_{id} \in LR_i$ is the revoked attribute's user's the algorithm output 0.

B. Correctness Analysis

In this section we proof the correctness analysis of matching index keywords search token outsource of file decryption as follow.
1)Correctness verification of matching between the encrypted index and trapdoor search.
$e\left(\prod_{j=1}^{D^{'}}(W_D, TK_{i,1}\right) = e\left(TK_{i,2}, W_{D^{'}}\right)$

$$= e(\prod_{j=1}^{D^{'}}(g^{t(r_1+r_2)}g^{H(W_j^{'})}, g^{\frac{ac\alpha}{t}})$$
$$= eg^{t(r_1+r_2)}g^{\sum_{j=1}^{D^{'}}H(W_j^{'})}, g^{\frac{ac\alpha}{t}})$$
$$= e(g,g)^{ac\alpha(r_1+r_2)}e(g,g)^{\frac{ac\alpha\sum_{j=1}^{D^{'}}H(W_j^{'})}{t}}$$
$$= e\left(TK_{i,2}, W_{D^{'}}\right)$$
$$= e(g^{r_1+r_2}\cdot\prod_{j=1}^{D^{'}}g^{\frac{H(W_j^{'})}{t}}, g^{ac\alpha})$$
$$= e(g^{r_1+r_2}\cdot g^{\sum_{j=1}^{D^{'}}\frac{H(W_j^{'})}{t}}, g^{ac\alpha})$$
$$= e(g,g)^{ac\alpha(r_1+r_2)}e(g,g)^{\frac{ac\alpha\sum_{j=1}^{D^{'}}H(W_j^{'})}{t}}$$

2)Correctness Verification of outsource decryption

$$= (E) = \frac{e(C_1\prod_{i\in I}C_{i,1}, D_{i,1})}{e(\prod_{i\in I}e(C_{i,2}, D_{i,2})}$$
$$= \frac{e(g,g)^{r_1 s}\prod_{i\in I}g^{-\alpha s_i r_1}, g^{(u-\omega_i)})}{e(\prod_{i\in I}g^{r_1\omega_i}, g^{(\gamma_i+\alpha s_i)})}$$
$$= \frac{e(g,g)^{r_1 s}e\prod_{i\in I}e(g,g)^{-\alpha u s_i r_1}\prod_{i\in I}e(g,g)^{\alpha\omega_i s_i r_1}}{\prod_{i\in I}e(g,g)^{r_1\gamma_i\omega_i}\prod_{i\in I}e(g,g)^{\alpha r_1 s_i\omega_i}}$$

$$E = \prod_{i \in I} e(g,g)^{-\alpha u s_i r_1}$$

3)Correctness of file decryption

$$msg = \frac{CT.e(C_{i,1},g)^{u+x}}{E}$$

$$msg = \frac{m.e(g,g)^{x\alpha s_i r_1}(g^{-\alpha s_i r_1},g)^{u+x}}{e(g,g)^{-\alpha u s_i r_1}}$$

$$msg = \frac{m.e(g,g)^{x\alpha s_i r_1}e(g,g)^{-\alpha u s_i r_1}e(g,g)^{x\alpha s_i r_1}}{e(g,g)^{-\alpha u s_i r_1}}$$

C. Security proof

We First consider the security of keyword index using security game indistinguishable against adaptive chosen keyword attack as follow.

Defination1: Decisional Linear assumption(DL): [26]

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

$$ADV^{A}_{Dln\,(\eta)} = \Pr[\mathcal{A}(1^{\kappa}), Par, D, R_0 = 1] - \Pr[A(1^{\kappa}), Par, D, R_1 = 1]$$

$Par = e(g,h,H,\mathbb{G}_1,\mathbb{G}_2)$, $D(h,g^b,g^c,g^{r_1},g^{r_2},h^{r_1+r_2},g^{a(r_1+r_2)})$ and $r_1,r_2,a,b,c \in \mathbb{Z}^*_P$
$R_0 = h^{r_1+r_2}, R_1 = g^{a(r_1+r_2)}$, $D = (h,g^b,g^c,g^{r_1},g^{r_2},h^{r_1+r_2},g^{a(r_1+r_2)})$ successfully distinguish is negligible in κwith non-negligible advantages where $g \in \mathbb{G}_1$and $R_0, R_1 \in \mathbb{G}_2$.

Defination2: Decisional Bilinear Diffie-Hellman Assumption(DBDH):

Let $\mathbb{G}_1$, $\mathbb{G}_2$ be two multiplicative group with group g and e is bilinear pairing map$a,b,c \in \mathbb{Z}^*_P$where
$g, g^a, g^b, g^c \in \mathbb{G}_1$ and g is generator of$\mathbb{G}_1$, $R \in \mathbb{G}_2$and the DBDH exist If for all PPT adversary $\mathcal{A}$ who can successfully distinguish tuple $(g, g^a, g^b, g^c, e(g,g)^{abc})$ from $(g, A, B, C, e(g,g)^R$ with non-negligible advantages withprobability$\frac{\varepsilon}{2}$.

$\Pr[\mathcal{A}(g,A,B,C,e(g,g)^{abc} = 1)] - \Pr[\mathcal{A}(g,A,B,C,R = 1)] = \frac{\varepsilon}{2}$

Theorem1: If DBDH hard problem then for all PPT adversaries has at most negligible advantages to break our system for chosen keywords attack with non-negligible advantages $\frac{\varepsilon}{2}$.

Proof: If there is polynomial time adversary $\mathcal{A}$ to break our VCP-ABE scheme with non-negligible advantages ε to get index keywords from the ciphertext we build a challenger $\mathcal{C}$ have the same non- negligible advantages $\frac{\varepsilon}{2}$.

The Challenger $\mathcal{C}$ run the setup algorithm for both the CA and each AA_k in the system to generate public key and master key send public key to the adversary flip a random bit $b \in (0,1)$ tuple . The challenger choose $a,b,c \in \mathbb{Z}_P$ and R$\in \mathbb{G}_2$ and transmit tuple if $b = 0$ then $(g, A, B, C, e(g,g)^{abc})$ if $b = 1$ then $(g, g^a, g^b, g^c, e(g,g)^R)$ and ask from the adversary to output $\theta \in (0,1)$ the challenger run the chosen keyword attack security game as follow.

(Init) The adversary submit theaccess structure $\mathbb{A}^*$, access policy $S^*$and unauthorized attribute's set L^*_i to be challenge through the challenger where challenger first run the setup algorithm.

(Setup)The challenger run the setup algorithm for both CA and each attribute authority AA_k and gives g to adversary. The adversary indicate a set of corrupt authorities $AA^*_C \subset AA_k$ as $(AA^*_C - AA_k) = Authn$ that is non corrupted thus for non-corrupt authority the challenger send the public key to the adversary and kept master key secret choose a bilinear map and publish public and master key. Randomly choose
$\alpha, \sigma \in \mathbb{Z}_P$ PK =(g,$\mathbb{G}_1$, e, $\mathbb{G}_2$, X, $\mathbb{H}$,$\{PK_{Li}\}$,$1 \le i \le k$] and $MK = (\alpha,\sigma), g^{\alpha}, 1 \le i \le k)$ and send the system parameter if and only if the authorities' is non-corrupt authorities.

Phase1 For the adversary $\mathcal{A}$ with challenge query challenger run the keyword generation algorithm initially generate an empty keyword index with following query from the adversary.

(Secret-Key-Query) The adversary submit L^*_k and $Sig(u^*_{id})$ query for secret key and certificate and ask adaptively $SK^*_{uid}\,L^*_1, SK^*_{uid}\,L^*_2, \ldots, SK^*_{uid}\,L^*_k$. The challenger first check the $Sig(u^*_{id})$ and authenticate with public key $PK_{CA}$of CA if the verification is successful the adversary win and get the secret key but $SK^*_{uid}\{u^*_{id} \neq u_{id}\}$ the u^*_{id} are not in the list of register and legal user's does not verify the certificate. Where the attribute set L^*_i with corresponding$\mathbb{A}^* = (M^*, \rho^*)$ and $L^*_i \not\subset \mathbb{A}$ the secret key does not match to access structure, it is due to the adversary query for secret key through corrupt attribute authority(AA^*_C) for the illegal attribute user's. Finally,

the challenger sends the secret key SK_{uid}^{*} to the adversary for the corrupt authority that is never match the legal and register authority attribute's user's secret key.

(Token-Query) The adversary want to generate trapdoor with secret key SK_{uid}^{*} for challenge keywords $W_D^{''}$ and submit to the challenger. Where The challenger randomly choose $\theta, \beta \in \mathbb{Z}_P$ and generate search token $TK_i^{*} = (TK_{i,1}, TK_{i,2}) TK_1 = \prod_{j=1}^{p'} g^{\theta} g^{H(\beta W_j^{'})}$, $TK_2 = g^{\beta\theta}$ as unauthorized user's.

The challenger responds from adversary the condition for the query trapdoor and interested keywords.

1)Only authorized legal users with u_{id}, secret key can generate the query keywords search trapdoor.

2)The adversary query trapdoor $SK_{ui}^{*}\left(q_{(\mathcal{A})}\right)^{(L_{ui}^{*})} = TK_i^{*}(q = j), j \in [1, w^{''}]$ for the interested keyword where $(q = j)$ if the adversary query search token match to the query keyword where TK_i^{*}does not match the search algorithm with query keywords and attribute's user's does not satisfy the access structure the challenger send token to adversary.

(Challenge) The adversary generate keywords set $W_D^{*} = g^{a\theta t} g^{H(\beta W_j^{'})}$ and output two keywords $W_0^{*}$and W_1^{*} send to the challenger. The challenger initially generate empty keyword index $W_D = g^{t(r_1+r_2)} g^{\beta H(W_j^{'})}$ and choose random bit $b \in (0,1)$ and encrypt $X = \prod_{i=1}^{k}(L_i, u_i) W_b$ with access structure $\mathbb{A}^{*}$ and access policy $\mathcal{S}^{*}$as:

$W_b = \{\mathbb{A}^{*}, e(g,g)^{abcH(W_j^{'})}, W_D^{''} = g^{st}, \forall L_{ui}^{*} \in \mathbb{A}^{*}\)$ where $s \in \mathbb{Z}_P^{*}$ If $b = 0$ then b_0: $(g, A, B, C, e(g,g)^{abc})$ send to the challenger $W_{b'}$ ciphertext denoted as:

$W_b^{*} = e(g,g)^{RH(W_j^{'})}, W_D^{''} = g^{st}, \forall L_{ui}^{*} \in \mathbb{A}^{*})$. The adversary view $s, a, b, c \in \mathbb{Z}_P^{*}$all are randomly chosen for simplicity $bc = a\theta t = s$ thus for further notion as:

$W_b^{*} = \{\mathbb{A}^{*}, e(g,g)^{sH(W_j^{'})}, W_D^{''} = g^{st}, \forall L_{ui}^{*} \in \mathbb{A}^{*}\)$ is according to adversary is valid keywords ciphertext for chosen keywords W_b under $\mathbb{A}^{*}$. Another way if $b = 1$ than b_1: $(g, g^a, g^b, g^c, R = e(g,g)^R)$ and send to the challenger. To get g from where R is randomly choose from $\mathbb{G}_2$ that leaks no information about W_b.

(Phase2)The adversary $\mathcal{A}$ adaptively query for secret key with the restriction and similar to phase1 that attribute's through corrupt authority for L_{ui}^{*} cannot verify the access structure and access policy and challenger respond to adversary similar to phase1.

(Gauss) The adversary output a gauss $b^{'}$of b if, $b = 0$ the adversary get valid tuple from challenger using DBDH assumption. The advantages of adversary to get keywords ciphertext information is ε and the probability to get $b = b^{'} = \frac{1}{2} + \varepsilon$. But $b \neq b^{'}$ the adversary output $b^{'} = 1$ the challenger send the random tuple to adversary the probability that $b = b^{'} = \frac{1}{2}$. The final advantage the adversary solve and break DBDH assumption is negligible with non-negligible advantages $\frac{\varepsilon}{2}$.

$= |\frac{1}{2}\Pr[\mathcal{A}|b = b^{'}|b = 0] + \frac{1}{2}\Pr[\mathcal{A}|b = b^{'}|b = 1] - \frac{\varepsilon}{2}|$

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

Theorem2: Our Proposed (VCP-ABE) scheme provide data confidentiality against unauthorized user's to that prevent Collison resistance to authorized user's.

Proof Let suppose there exist L_{iu}^{*}unauthorized attributes user's such that $\sum_{i \in L_{iu}^{*}} \gamma_i \omega_i = (1,0,\ldots,0)$using LSSS scheme. For unauthorized user's it necessary to compute and verify his legality and identification from attribute authority to generate key and access data$e(\varphi, g) = e(SigH(uid).g^{\pi})^{u_i}, PK_{CA})$ where different users have different identities that cannot match to unauthorized and illegal user's identity with register and verified user's $SigH(uid)$. The unauthorized user's does not have the same attribute corresponding to row i of matrix it unable to compute vector $< \omega_i >$ with $\sum_{i \in L_{iu}^{*}} \gamma_i \omega_i = (1,0,\ldots,0)$. Further it does not calculate the $e(g,g)^{s}$ where s share of secret for the authorized attribute's user's. In attribute's revocation only non-revoked attribute can get his secret key from attribute authority as $X^{'} = \prod_{i=1}^{k}(LR_i^{'}, u_i{'})$ where the central authority remove the revoke attribute's user's with corresponding identity $g^{\alpha^{'}} H(uid^{'}).^{u_i}$ the revoked user's does not receive the secret key from the authority to acquire the content key and the secret key to access the data owner update data further.

V. Performance Analysis Theoretical Analysis Of Our (VCP-ABE) Scheme.

In this section we use some of the variables for the complexity computation in which $\mathbb{L}$ is the number of least attribute set that satisfy the access structure for specified access policy, L_{ui} the number of attribute user's that satisfy the access structure, $L_{uR_i^{'}}$ is the number of non-revoked attribute's user's. where P is paring operation $(E_1, m^{'})$ is exponential and multiplication operation in group $\mathbb{G}_1$. Similarly (E_2, m^{*}) is exponential and multiplication operation in group $\mathbb{G}_2$ while j is number of encrypted and interested keywords search. we

compare our (VCP-ABE) scheme with others scheme in term of performance analysis and computational complexity analysis of some characteristic and efficiency difference of our scheme in literature [16,17,20,21,22] in table2 and table3 as follow.

The scheme in table2 [16,17,21] cannot support multiple authority, the scheme [16,17] ciphertext policy attribute based encryption but not verifiable and cannot support large universe where [20] is ABE and cannot support large universe. Similarly, the scheme [17,20,21] not apply his scheme for interested keyword search the advantages is that our scheme supports efficient and secure keyword's search on the encrypted keywords index with multiple authority. Where our scheme supports efficient attribute's user's revocation the scheme [16,17,20,21,22] in table2 cannot support attribute's user's revocation. To compare our scheme in table3 the scheme [20,21] not allow to search in interested keyword's finally our scheme support attribute's revocation that are connected to update the secret key and ciphertextwhere the schemes [16,17,20,21] in table3 cannot support.

Tabel2 Performance analysis comparison of our scheme

	Our	[16]	[17]	[20]	[21]
Multiple-authority	Yes	NO	NO	Yes	NO
Verifiability	Yes	NO	NO	Yes	Yes
CP-ABE	Yes	Yes	Yes	NO	Yes
Keyword-search	Yes	Yes	NO	NO	NO
Revocation	Yes	NO	NO	NO	NO
Access policy	Yes	Yes	Yes	Yes	Yes
Security	CKA	CKA	CPA	CPA	CPA
Large universe	Yes	NO	NO	Yes	NO

Table3 Computation complexity comparison analysis of our scheme

	Our	[20]	[21]	[22]
Setup	$O(L_{ui})E_1 + O(1)P$	$(L_{ui}+2)E_1 + 2P$	$(L_{ui}+1)E_1 + P$	$(L_{ui}+4)E_1$
Key-Gen	$(L_{ui}+4)E_1 + 3P$	$(L_{ui}+3)E_1$	$(2L_{ui}+2)E_1$	$(L_{ui}+6)P$
Encryption	$(L_{ui}+9+j)E_1 + m' + E_2$	$(7L_i+7)E_1$	$(2L_i+1)P + 3L_{ui}E_2$	$(L_{ui}+j+6)E + E_2$
Token-Gen	$(j+2)P + 3E_1 + 2E_2$	$(L_{ui}+3)E_1 + 3P$	$(2L_{ui}+1)P$	$(L_{ui}+4)E_1 + 4P$
Search	$(j+3)P + 3m^*$	……	……	$(j+3)P + 2m^*$
Decryption	$2P + 3m^* + 3E_2$	$(4L_{ui}+2)P + E_2 + m^*$	$L_{ui}E_1$	$P + 3E_1 + 3m^*$
Key-Update	$O\left(L_{uR_i'}\right)E_1 + L_{uR_i'}P$	……	……	……
CP-Update	$O\left(L_{uR_i'}\right)E_1 + O\left(L_{uR_i'}\right)P$	……	……	……

VI. Conclusion

In this paper, we proposed large universe, multiple authority (VCP-ABE) scheme for fine grained data access control with keyword search that support attribute's revocation, outsource encryption, decryption, and correctness verification of updating ciphertext simultaneously. The authorized attribute users are able to get the secret key, retrieval keys from corresponding authority after the verification of certificate for keywords search and ciphertext decryption. The data owner encrypts his data using any Boolean Formula over set of attribute's chosen from each attribute authority. In ourscheme only non-revoked attribute's users can update his\her secret key through trusted authority that enables attribute users in efficient decryption for new encrypted and updated data. The revoked user's cannot able to combine his secret key information using his revoke identity and old key's to update his secret key that prevent collision attack with distinct identity of identifiers. We introduce the CPS for the outsource encryption, outsource decryption and the correctness of ciphertext update verification after the non-revoked user's secret key update without learn any secret information. The most critically our scheme security for data confidentiality and selective keywords attack has been proven under the complexity assumption of standard group model. Further we provide the details of performance analysis with security analysis for our design scheme.

Acknowledgments

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 revivers, which improved the presentation.

References

[1]. Sahai A, Water B, Fuzzy identity-based encryption Proc. 24 Annual Int. Conf. Theory and Application of Cryptographic Techniques advance in Cryptography Eurocrypt, Lecturer notes in computer science Springer (2005) 3494:457-473.

[2]. Goyal V, Pandy O,Sahai A, and Water B, Attribute-based encryption for fine-grained access control of encrypted data. in proceeding of 13th ACM conference on computer and communications security (ACM 06) 2006:89-98.

[3]. Bethencourt J, Sahai A, and Water B, Ciphertext policy attribute-based encryption scheme. in proceeding IEEE Symposium on security and privacy.Berkely, 2007, 321-334.

[4]. Chase M, 2007 Multi Authority Attribute-based encryption Proc. 4th Theory of Cryptography Conf. TCC Lecture Notes in computer science Springer. 2007 4392:515-534.

[5]. Chase M, and Chow S.S.M., Improving Privacy and Security in Multi-Authority Attribute-based Encryption. Proc. ACM Conf. Computer and Communication Security, ACM, CCS. 2009, 121-130.

[6]. Attrapadung H, and Imai H, Attribute-based Encryption Supporting Direct/Indirect Revocation Modes. Proc. 12th IMA Int. Conf. Cryptography and coding Lecture Notes Computer Science. Springer, 2009, 5921: 278-300.

[7]. Zheng Q, Xu S, and Ateniese G, "VABKS. Verifiable Attribute based Keyword Search Over Outsource Encrypted Data. In IEEE INFOCOM, 2014, 522-530. Doi10.1109/INFOCOM.2014.6847976

[8]. Sun W. Yu, S. Lou W, Hou Y.T, and Li H, 2014 Protecting your right: Attribute-based keyword search with fine-grained owner-enforced search authorization in the Cloud Computing. In Proceeding of the IEEE INFOCOM 2014-Conference on Computer Science and Communication, 2014, 226-234.

[9]. Wang H, Dong X, and Cao Z, Multi Value Independent Ciphertext Policy Attribute-based Encryption with Fast Keyword Search. IEEE Trans. Serv. Comput. 2017. doi:10.1109/TSC.2017.2753231

[10]. Ostrovsky Sahai A, and Water B,Attribute-based encryption with non-monotonic access structure In proceeding of 14th ACM.Conference on Computer and communication Security. 2007, 195-203.

[11]. Doshi N, and Jinwala D.C, Fully Secure Ciphertext Policy Attribute-based Encryption with Constant length Ciphertext and Faster Decryption. Secur. Commun. Netw. 2014, 7:1988-2002. https://doi.org/10.1002/sec.913

[12]. Yang K. Jia X, Attribute-based Access Control for Multi-Authority System in Cloud Storage In: 32nd International Conference on Distributed Computing IEEE. 2012, 536-545.

[13]. Yang K,Jia X, Ren K, Chang B, and Xia R, DAC-MACS Effective Data Access Control for Multi Authority Cloud Storage System. IEEE Trans. Inf. Forensics Secur. 2013, 8(11):1790-1801.

[14]. Yang K, Jia X, and Ren K, Attribute-based fine-grained access Control with efficient Revocation in Cloud Storage. In proceeding of the 8th ACM SIGSAC Symposium on information, Computer Communication Security ACM, 2013, 523-528.

[15]. Chen C, Chen J, Lim H.W, Zhang Z, Feng D, Ling S, and Wang H,Fully Secure Attribute-Based System with Short Ciphertext\Signature and Threshold Access Structure. in Cryptographic Track with at the RSA Conference. Springer 2013, 50-67.

[16]. Qiu S, Liu, J. Shi Y, and Zhang R, Hidden Access Policy Ciphertext Policy Attribute-based Encryption with keywords Search against keywords guessing attack. Sci. China Inf. Sci. 2017,60:052105DOi: 10.1007/s11432-015-5449-9

[17]. Cui H, Deng R.H, Wu G, Lai J, Yi X, and Nepal S, An Efficient an expressive Ciphertext policy attribute-based encryption scheme with partially hidden access structures. Comput. Netw. March 2018, 133:157-165. DOi: https://doi.org/10.1016/j.comnet.2018.01.034

[18]. Wang S, Yao L, and Zhang Y, Attribute-based encryption with multi keywords search and Supporting attribute revocation in cloud storage. PLoS ONE,2018,https://doi.org/10.1371/journal.pone.0205675

[19]. Yin H, Zhang J, Xiong Y, Ou L, Li F, Liao S, and Li K,CP-ABSE A Ciphertext Policy Attribute-based Searchable Encryption Scheme. IEEE Access 2019. 7:5682-5694.DOi: 10.1109/ACCESS.2018.2889754

[20]. Lai J, Deng R.H, Guan C, and Weng J, Attribute-based Encryption with verifiable outsource decryption. IEEE Trans. Inf. Forensics Secur. Aug-2013, 8 :1343-1354.

[21]. Zhang K, Ma J, Liu J, and Li H, adaptively secure multi authority attribute encryption scheme with Verifiable outsource decryption. Sci. China Inf. Sci., Aug 9-2016,59 099105:1–099105Doi: 10.1007/s11432-016-0012-9.

[22]. Wang S, Jia S, and Zhang Y, Verifiable and multi-keyword searchable attribute-based encryption scheme for cloud storage. IEEE Access (2019) ,7:50136-50147.

[23]. Xiong H, and Sun J. Comments on verifiable and Exculpable Outsource Attribute-based Encryption for the Access Control in Cloud Computing. IEEE Depend, Secure. 14:461-462.Doi:10.1109/TDSC.2015.2499755 (2017),

[24]. Ding S, Li C, and Li H, A Novel Pairing free CP-ABE Based on Elliptic curve cryptography for IOT. DOi: 10.1109/ACCESS.2018.2836350. 15-May-2018, 6:27336-27345.

[25]. Waters B, Ciphertext Policy attribute-base encryption scheme an Expressive, Efficient and Provable Secure Realization. in: Public Key Cryptography 14th international Conference on Practice and Theory Cryptography Proceeding in Lecturer Notes in Computer Science March 6-9-2011, 6571: 53-70.

[26]. Agrawal S, and Chase M, FAME: fast attribute-based message encryption ACM, DOi:10.1145/3133956.3134014(2017), 665-682.

Muqadar Ali. "A Verifiable Ciphertext Policy Attribute-Based Encryption(VCP-ABE) Scheme with Keywords Search and Revocation." IOSR Journal of Mathematics (IOSR-JM) 15.5 (2019): 21-33.