ISSN:0975-9646

Protecting User Privacy By Using Decentralized Key-Policy Attribute-Based Encryption

Kishor B.Badade, Dr.S.S.Lomte, R.A.Auti

Department of CSE, Everest College of Engineering
Aurangabad [M.S], India

Abstract- **Decentralized key policy ABE where each authority can issue the secret key to user independently without any co-operation of a central authority. It means that that there is no need to trust on to the central authority due to this even if multiple authorities are corrupted they can't collect the users attributes by tracing users GID. In decentralized key-attribute based encryption both the user secret key and the ciphertext are label with set of different attribute. Message can be encrypt under set of attribute so if anyone want the decrypt the ciphertext the receiver must obtain data only when there is match between his secret key and attribute listed in the ciphertext. In multi authority ABE secret key of different users from different authorities must be tied to his global identifier (GID). To avoid collagen attack this is not efficient to protect the users privacy.**

So we propose Decentralized key policy ABE scheme to protect the users privacy in this scheme each authority can issue secrete key to users separately without having any idea of his GID. This scheme required standard complexity assumption e.g. (Decisional by linear deffie-Hellman) dbdh instead of non standard complexity assumption (e.g., *q*-decisional Diffie-Hellman inversion) which is used in previous scheme.

Keywords- **Attribute based encryption multi authority, privacy.**

I. INTRODUCTION

Secret writing is hot people doing from last several years. In Greek that secret writing is known as “Kryptos” (secret) “Grapho” (writing) that is known as cryptography in English language the cryptography deals with encryption and decryption. The history of cryptography is 1975 dealing with encryption i.e. encoding plaintext into ciphertext and decryption is the reverse of encryption.

Sze-ming chow [1] introduce the evolution of encryption as follows from secret key encryption to public key encryption. From public key encryption to identity based encryption. From identity based encryption to attribute based encryption, in traditional access control a central authority handle all users access to sensitive data [2]. There are two problem especially in distributed system first is a users identity needs to be a validated by the authority. In large distributed system it is a difficult task to manage numerous users' identity. The one is total user must trust on to a central authority if the authority is catty you can act like any user without being detected. Another scheme that is attribute based access control are capable to share data with multiple users without inform their identities. The attribute based access control [3][4]. In this scheme allow user to be approve by the descriptive attribute in place of their unique identities user can share his data by determines an access structure so all the users whose attribute satisfy it can access data without informed their identities in order to minimize trust on central authority some decentralized and distributed access control scheme are purposed [6]. Decentralized attribute based access control schemes demonstrated lots of matrix irregularly consider the users privacy to give the very good solution for sharing the sensitive data with the more than one user in distributed system and the protect the user privacy. A decentralized attribute based access control scheme should be addressed. In day to day communication environment the confidential data must be encrypted before transmitted the transactional encryption scheme can't express composite access policy and a sender known all the public key of the receiver attribute based encryption introduced by sahai and waters [4] is a more capable encryption schemes and it can express composite access structure. In an attribute based encryption scheme. Both users secrete key and ciphertext are labelled with set of attributes the basic concept of ABE is to construct a fuzzy identity base encryption IBE scheme [8][9][10] basically there are two kind of attribute based encryption scheme as give below.

Key-policy ABE (KP-ABE): in this scheme the secret key are associated with an access structure while the ciphertext is label with set of attributes [4][13].

Ciphertext-policy ABE (CP-ABE): in this scheme the ciphertext is associated with an access structure while the secret key are label with a set of attributes [14][15][16].

The first CP-ABE scheme was purpose by be then court et al[3] and it was prone to be a secure in generic group model in comparison with KP-ABE. The access structure CP-ABE determine by the enryptor instead of central authority. So the enryptor can decide who will decrypt the ciphertext and in other this is decide by CA in in the PK-ABE scheme. Nawpar and cheung purposed another CP-ABE scheme [14] and minimize the problem of braking their scheme to the decisional by linear define Hellman assumption these CP-ABE scheme can only expressed threshold access structure. The dual policy ABE scheme [19] purposed by attrapadung and lmai that put together the KP-ABE scheme with CP-ABE scheme here to access structure are created one is for subjective attribute held by user other is objective attribute level with ciphertext. Again there is only one access structure in both KP-ABE and CP-ABE scheme. Real and but rialbart preneel [20] purpose a blind key extract protocol for centralized ABE so this scheme constitute a blind centralized ABE scheme.

1.1 Multiple Authority Attribute Encryption:

where the secret keys can come from multiple authorities this question is left by sahai and water[4] chase gives response to this question by proposing a multi authority KP-ABE scheme [5] number of authority are there one authority called as central authority who knows the secret keys of the other authorities so all the user need to obtain secret keys from all these authorities it is difficult to prevent collision attacks in multi authority ABE schemes.

Chase[5] over came this difficulty by introducing the global identifier (GID) all the user secret keys from different authorities must be tied to his GID in order to let the ciphertext be independent of the users GID this scheme is not a decentralized ABE scheme chase made and important steps from one authority ABE to multi authority ABE again chase and chow purposed multi authority KP-ABE scheme [13] which is improved the previous scheme[5] and removed the need the central authority but in previous multi authority ABE scheme \[5] all user must submit their GID to each authority to obtain the corresponding secret keys in this case the user being stress by a group of corrupted authorities.

Chase and chow provided and anonymous key issuing protocol for the GID in which the two party secure computation technique is employed in this a group authorities not co-operate to pull the users attributes by stressing his GID. After all multiple authority must collaborate to set of a system each pair of authorities must execute a to party to key exchange protocol to share seed of the selected pseudorandom function[30]. Lekwo and water purpose a new multi authority ABE scheme i.e. the decentralizing CP-ABE scheme[6] in this scheme there is no co-operation between multiple authorities is required in the setup stage. And a key generation stage the there is no central authority. The authority in this scheme join or live system freely without re initializing this scheme is inefficient because attribute of the user can collected by tracing his GID. Liu et al introduce a fully secure multi authority CP-ABE scheme[22]. This scheme best on CP-ABE scheme [16] there are different central authority and attribute authorities. The authorities who in the central position issue identity related key to user and attribute authorities issue attribute related key to user. This scheme is also design in a composite order [N=p1,p2…pn] by linear group.

Li et al[7] purposed a multi authority cipher policy ABE scheme with accountability where the anonymous key issuing protocol was employed in this scheme the user can only obtain a secret key anonymously from n-1 authorities he can be traced when he shared his secrete key with other. This scheme relied on DBDH, DLIN, qDDHI assumption.

A. Our Contribution

Here we are using decentralized key policy ABE scheme to protect the users privacy this scheme is for giving a privacy to multiple authority and each and every authorities can issue a secrete key to users with the help of attribute based encryption we are storing users secrete key and ciphertext are labelled with set of attributes. Protecting users privacy is an important issue so our decentralized KP-ABE can be used as a sound solution for secure data transfer which can improve the privacy.

In our scheme each authority can provide a secrete key to user separately without having any idea about his global identifier. Here the multiple authorities can work independently without any co-operation so if numbers of authorities are curpted they cannot collect the users attribute by tracing his global identifier. Our scheme is best on standard complicity assumption DBDH in place of non standard complexity assumption.

II. Related Work

A. Fuzzy Identity Based Encryption by Amit Sahai and Brent Waters [4]. They introduce a new type of identity based encryption IBE scheme that they call fuzzy identity based encryption in this they view an identity as a set of description attributes.

A fuzzy IBE scheme can be applied to enable encryption using biometric input as identities. The error to learners property of fuzzy identity based scheme is precisely what allows for the use of biometric identities which inherently will have a some noise each time they are sampled additionally they show that the fuzzy identity based encryption can be used for a type application this work motivate a few interesting open problem the first is whether it is possible to create a fuzzy identity scheme where the attribute came from multiple authorities while it is natural for one authority to certify all attribute that compromise a biometric.

B. Fully Secure Functional Encryption And Hierarchical Inner Product Encryption Attribute Based Encryption by lewko, T. Okamto, A. Sahai, K. Takashima and B. Water [16].

In this paper they present two fully secure functional encryption scheme the first result is fully secure based encryption ABE scheme previous construction of ABE were only proven to be selectively secure the scheme achieve a fully security by adapting the dual system encryption methodology introduce by water to obtain a fully secure IBE and HIBE system the primary challenges in applying in dual system encryption to ABE is the richer structure of key and ciphertext in an IBE or HIBE system. A key and ciphertext are both associate with the same type of simple object identities in an ABE system. Key and ciphertext are associated with more complex object attribute and access formula. This system construct in Composite order by linear group were the order is product of three prime the scheme support arbitrary monatomic access formula. The second result fully secure predicate encryption scheme for inner product predicates as for ABE previous construction of such a scheme where only proven to be a selectively secure security is proven under non interactive assumption whose size do not depend on the number of queries the scheme also present fully hierarchical predicate encryption scheme under the same assumption.

C. *Ciphertext-Policy Attribute-Based Encryption An Expensive, Efficient, And Provably Secure Realization* by B. Water [17].

The scheme presents a new methodology for realizing a ciphertext-policy attribute-based encryption CP-ABE under concrete and non interactive cryptography assumption in the standard model. The solution allows any enryptor to specify access control in terms of any access formula over the attribute in the system. In this system ciphertext size encryption and decryption time scales linearly with the complexity of the access formula the only previous work to achieve these parameter was limited to proof. In the generic group model the scheme present a three construction within a framework the first system is proven a selectively secure under a assumption that they call decisional parallel bilinear Diffie-Hellman Exponent PBDHE assumption. This can be viewed as generalization of the BDHE assumption.

D. Decentralizing Attribute Based Encryption By A. Lewko And B. Water [6].

They proposed multi authority attribute based encryption system here any party can become an authority and there is no requirement for any global co-ordination other than they creation of an initial set of a common reference parameter a party can simply act as an ABE authority by creating a public key and assuming a private key to different user. That reflect their attribute a user can encrypt data in terms of any Boolean formula over the attribute issued for any chosen set of authorities. In construction this system the largest technical harder is to make it collision resistant prior attribute based encryption system achieved collision resistant when the attribute based encryption system. Authority tied together different component of a user private key bi a randomizing the key however in the system each component came from a potentially different authority.

III. Preliminaries

In this paper we denote that x is randomly selected from X, especially by $x \xleftarrow{R} X,$ here x selected from X identically if X is finite set so we can say that $\in: Z \rightarrow R$ is negligible, if for all $z \in Z$ there exists a value $\eta \in Z$ such that $\in(x) < \frac{1}{x^z}$ for all x > η. By R $\xleftarrow{s}$ S and R $\xrightarrow{r}$ S, we denote that party S sends s to party R and party R sends r to party S, respectively. We denot $\mathbf{KG}\left(1^{\ell}\right)$ as the secret-public key generation algorithm where ℓ the security parameter is if X is a finite set, by |X|, we denote the cardinality of X. By A(x) → y, we denote that y is computed by running algorithm A on input x. Suppose that z_p is a finite field with prime order p, by z_p [x], we denote the polynomial ring on z_p, which consists of all polynomials with coefficients from z_p.

A. Building Blocks

In this paper, the following building blocks are used Lagrange Interpolation. Suppose that $p(x) \in z_p [x]$ is a ($k-1$) degree polynomial. Given k different polynomial values p($x1$), p($x2$), …. , $p(x_k)$, the polynomial p(x) can be reconstructed as follows:

p(x)
=

$$p(x) = \sum_{x_i \in S} p(x_i) \prod_{x_j \in S x_j \neq, x_i} \frac{x - x_j}{x_i - x_j} = \sum_{x_i \in S} p(x_i) □ x_i, s(x)$$

where S = {xi, $x2$,… x_k }. The Lagrange coefficient for x_i in S is $□ s_i, s(s) = \prod_{x_j \in S x_j \neq, x_i} \frac{x - x_j}{x_i - x_j}$ Therefore, given any k different values $p(x1)$, $p(x2)$,… , $p(x_k)$, we can compute p(x) for $\forall x \in Z_p$ However, when only $k-1$ different polynomial values are provided, the other polynomial values are unconditionally hidden.

Commitment. A commitment scheme consists of tree algorithms: C = (Setup, Commit, Decommit).

- Setup(1^{ℓ}) → *params*. This algorithm takes as input a security parameters ℓ and outputs the system parameters *params*.
- Commit*(params,M)* → *(com, decom)*. This algorithm takes as input the parameters *params* and a message *M* and outputs a commitment com and a decommitment *decom*. *decom* can be used to decommite the commitment *com*.
- Decommit*(params,M, com, decom)* → {0, 1}. This algorithm takes as input the parameter *params*, the message *M*, the commitment com and the decommitment *decom* and outputs 1 if *decom* can decommite *com* to *M;* Otherwise, this algorithm outputs 0.

A commitment scheme should satisfy two properties: hiding and binding. The hiding property requires that the message M keeps undisclosed until the user reveals it. The binding property requires that only one value *decom* can be used to decommit the commitment.

We use the Pedersen commitment scheme which is a perfectly hiding commitment scheme and is based on the discrete logarithm assumption. Let G be a prime order group with generators g0, g1, g2, … , gl. In order to commit messages (m1,m2,…,ml), the user selects r $\xleftarrow{R}$ Zp, and computes the commitment $T = g_0^r \prod_{j=1}^{l} g_j^{mj}$. The user can use r to decommit the commitment later.

Proof of Knowledge: We use the notation introduced by Camenisch and Stadler [23] to prove statements about discrete logarithm. By *PoK{(α, β, γ) : y =* $g^{\alpha} h^{\beta} \wedge \tilde{y}^{\alpha} \tilde{h}^{\gamma}$ *}* we denote a zero knowledge proof of knowledge of integers α, β, and γ such that $y = g^{\alpha} h^{\beta}$ and $\tilde{y} = \tilde{y}^{\alpha} \tilde{h}^{\gamma}$ hold simultaneously in groups G = <g> = <h> and G˜ = <g˜> = <h˜>. Conventionally, the values in the parenthesis denote the knowledge that is being proven, while the rest of the other values are known to the verifier. There exists a knowledge extractor which can be used to rewind these quantities from a successful proves.

B. Decentralized Key-Policy Attribute-Based Encryption
The Formal Definition Of Access Structure Is As Follows:

Definition 1. (Access Control) [18]. *Let* P = {*P1, P2, ...,PN*} *be a set of parties. A collection* $A \subseteq 2^{\{P1,P2,\cdots,PN\}}$ *is monotonic, if* $S_1 \in A$ *and* $S_1 \subseteq S_2$ *implies* $S_2 \in A$. *An access structure (resp., monotonic access structure) is a collection (resp., monotonic collection)* A *of non-empty subsets*
of {*P1, P2, ... , PN*}, *namely* $A \subseteq 2^{\{P1,P2,\cdots,PN\}} \setminus \{\varphi\}$. *The sets in* A *are called the unauthorized sets, and the sets outside of* A *are called the unauthorized sets.*

A decentralized KP-ABE scheme consists of the following five algorithms:[28]

- Global Setup(1^{ℓ}) → *params*. This algorithm takes as input a security parameter _ and outputs the system parameters *params*.
- Authority Setup(1^{ℓ}) → *(SK$_i$, PK$_i$,A$_i$)*. Each authority A_i generates his secret-public key pair *KG(*1^{ℓ}*)* → *(SK$_i$, PK$_i$,A$_i$)* and an access structure A_i, for *i =1, 2, ...,N.*
- KeyGen*(SK$_i$,GID, A$_i$GID)* → *SK$_i$U* . Each authority A_i takes as input his secret key SK_i, a global identifier *GID* and a set of attributes A_i *GID*, and outputs the secret keys $SK^i{}_U$, where $A^i{}_{GID} = A_{GID} \cap A^{\sim}{}_i$, A_{GID} and $A^{\sim}{}_i$ denote the attributes corresponding to the *GID* and monitored by A_i, respectively.
- Encryption *(params,M,AC)* → *CT*. This algorithm takes as input the system parameters *params*, a message *M* and a set of attributes A_C, and outputs the ciphertext *CT*, where $A_c = \{A_c^1 A_c^2 .... A_c^N\} and A_c^i = A_c \cap A_C^{\sim}$ and A_i
- Decryption *(GID,{SK$^i{}_u$}i∈I$_C$,CT)* This algorithm takes as input the global identifier *GID*, the secret keys *{SK$^i{}_u$}i∈I$_C$* and the ciphertext *CT*, and outputs the message *M*, where I_C is the index set of the authorities A_i such that $A^i{}_c \neq \{\varphi\}$.

Definition 2. *We say that a decentralized key-policy attribute-based encryption scheme is correct if*

$$\left[\text{Decryption(GID},\{\text{SK}_U^i\}\text{i} \in \text{IC,CT)= M} \;\middle|\; \begin{array}{l} \text{Global Setup } (1^{\ell}) \to \text{params;} \\ \text{Authorities Setup } (1^{\ell}) \to (SK_i, PK_i, A_i); \\ \text{KeyGen } (SK_i, GID, A_{GID}^i) \\ \text{Encryption(params,M, AC)} \to \text{CT;} \\ \{\text{A}_{GID} \cap A_i^{\sim} \in A_i\}_i \in I_C \end{array} \right]$$

where the probability is taken over the random coins of all the algorithms in the protocol.

Security Model

Our security model on the decentralized ABE is similar to the model proposed in [5], [13], which is known as the selective-set model. This model is described as follows:

Initialization: The adversary A submits a set of attributes AC which he wants to be challenged and a list of corrupted authorities C_A, where $|C_A| < N$. There should exist at least one authority A_j such that $A_C \cap A^{\sim}{}_j \notin A_j$.

Global Setup: The challenger runs the Global Setup algorithm to generate the system parameters *params,* and sends them to *A*.

Authority setup:

1) For $A_i \in C_A$, the challenger sends the secret-public key pair *(SK$_i$, PK$_i$)* to *A*.

2) For $A_i \notin C_A$, the challenger sends the public key PK_i to *A*.

Phase 1: The adversary *A* can query secret keys for sets of attributes $A^*{}_{GID1}$, $A^*{}_{GID2}$,..., $A^*{}_{GIDq1}$, the only constraint is $A_C \not\subset A^*{}_{GIDi}$ for *i = 1, 2, ..., q1*.

Challenge: A submits two messages *M0* and *M1* with equal length. The challenger flips an unbiased coin with {0, 1}, and obtain *b* ϵ {0, 1}. The challenger computes *CT** = Encryption*(params,M$_b$,A$_C$)* and sends *CT** to *A*.

Phase 2: The adversary *A* can query secret keys for sets of attributes $A^*{}_{GIDq+1}$, $A^*{}_{GIDq+2}$,... $A^*{}_{GIDq}$ Phase 1 is repeated.

Guess: The adversary *A* outputs his guess *b'* on *b*.

Definition3: A decentralized key-policy attribute-based encryption (DKP-ABE) scheme is (T, q, ϵ) secure in the selective-set model if no probabilistic polynomial-time adversary A making q secret key queries has advantage at least $Adv_A^{DKP-ABE} = |\Pr[b' = b] - \frac{1}{2}| > \in(\ell)$ in the selective-set model.

C. Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption[28]

We have described the decentralized KP-ABE scheme and its security model. The privacy-preserving decentralized KP-ABE scheme has the same algorithms Global Setup, Authority Setup, Encryption and Decryption with the decentralized KP-ABE scheme. We only replace the algorithm KeyGen in the decentralized KP-ABE scheme with algorithm BlindKeyGen. In a privacy-preserving decentralized KP-ABE scheme, the authorities do not know the user's GID nor can cause failures using the information of the GID. This concept is from blind IBE schemes [24], [25]. We define this algorithm as follows:

BlindKeyGen*(U(params, PK$_i$,GID, decom)* ↔ *A$_i$(params, SK$_i$, PK$_i$,A$_i$, com))* → *(SK$_i$U , empty)*. In this algorithm, the user *U* runs the commitment algorithm Commit*(params,GID)* → *(com, decom)* and sends com to the authority A_i. Then, the user *U* and the authority A_i take as input *(params, PK$_i$, GID, decom)* and *(params, SK$_i$, PK$_i$,A$_i$, com)*, respectively. If Decommit*(params,GID, com, decom)* → *1*, this algorithm outputs a secret key *SK$_i$U* for U and empty for A_i. Otherwise it outputs error messages (⊥,⊥) for both *U* and A_i.

The algorithm BlindKeyGen should satisfy the following two properties: leak-freeness and selective-failure blindness [24], [25]. Leak-freeness requires that, by executing algorithm BlindKeyGen with the honest authorities, the malicious user cannot know anything which he cannot learn by executing algorithm KeyGen with the honest authorities. Selective-failure blindness requires that the malicious authorities cannot know anything about the user's GID and cannot cause the algorithm BlindKeyGen to selectively fail

depending on the user's choice of GID. We use the following two games to define these two properties.
Leak-freeness: This game is defined by the real experiment and the ideal experiment:

Real Experiment: Runs Setup(1^{ℓ}) → params and Authority Setup(1^{ℓ}) → *(SK$_i$, PK$_i$,A$_i$)*. As many times as the distinguisher *D* wants, the adversary *U* chooses a *GID* and executes the algorithm BlindKeyGen with the authority A_i: BlindKeyGen*(U(params, PK$_i$,GID, decom)* ↔ *A$_i$ (params, SK$_i$, PK$_i$,A$_i$, com))*.

Ideal Experiment: Runs Setup(1^{ℓ}) → *params* and Authority Setup(1^{ℓ}) → *(SK$_i$, PK$_i$,A$_i$)*. As many times as the distinguisher *D* wants, the simulator Û chooses a *GID* and queries a trusted party to obtain the output of the algorithm KeyGen*(SK$_i$,GID,A$_i$ GID)* if Decommit*(params,GID, com, decom)* → *1*, and ⊥ otherwise.

D. Complexity Assumption:

Let G and G_τ be two multiplicative cyclic groups with prime order p, and g be a generator of G. A bilinear map $e : G \times G \to G_\tau$ is a map with following properties:
1) Bilinearity. for all $x, y \in G$ and $u, v \in Z_p$, $e(x^u, y^v) = e(x, y)^{uv}$.
2) Non-degeneracy. $e(g, g) \neq 1$, where 1 is the identity of G_τ.
3) Computability. There exists an efficient algorithm to compute $e(x, y)$ for all $x, y \in G$.

Let $GG(1^{\ell})$ be a bilinear group generator which takes as input a security parameter ℓ and outputs the bilinear group (e, p, G, G_τ) with prime order p and *a* bilinear map $e: G \times G \to G_\tau$.
Definition7. (Decisional Bilinear Diffie-Hellman (DBDH) Assumption)[8]. *Let a, b, c, z R←*

Z_p, $GG(1^{\ell}) \to (e, p, G, G_\tau)$, and g *be a generator of* G. *The DBDH assumption holds in (e, p, G, G_τ), if no probabilistic polynomial-time adversary* A *can distinguish* (A,B,C,Z) = $(g^a, g^b, g^c, e(g, g)^{abc})$ *from* (A, B,C,Z) = $(g^a, g^b, g^c, e(g, g)^z)$ *with advantage*

$$Adv_A^{DBDH} = \left| \begin{array}{l} \Pr\left[A(A,B,C,e(g,g)^{abc}) = 1 \right] \\ - \Pr\left[A(A,B,C,e(g,g)^{z}) = 1 \right] \end{array} \right| > \in (\ell)$$

where the probability is taken over the random choice of a, b, c, z $\xleftarrow{R}$ Z_p, *and the bits consumed by* A.

IV. Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption

In this section, we propose a decentralized KP-ABE scheme based on the DBDH assumption. Then, we describe a privacy-preserving extract protocol for the secret keys. In our privacy-preserving decentralized KP-ABE scheme, a user executes a 2-party secure computation protocol with an authority to obtain his secret keys. As a result, the user can obtain his secret keys anonymously without releasing anything about his identifier to the multiple authorities. As pointed in [13], an anonymous credential system [26], [27] can be used by the user to convince the authorities that he holds the corresponding attributes without revealing his identifier. In an anonymous credential system, a user can obtain a credential and prove the possession anonymously. The user can interact with different partners with different pseudonyms [28] such that no partner can link the pseudonyms to the same user. Furthermore, the user can prove that he has obtained multiple credentials which correspond to the same identifier without revealing it. Hence, this technique can be employed in our system to allow the user to obtain the corresponding secret keys without revealing his identifier to the authorities.

A. Decentralized Key-Policy Attribute-based Encryption

This idea is inspired by the IBE schemes [11], [12] and the multi-authority ABE schemes [5], [13].
Overview: In our scheme, suppose that there are N authorities $A_1, A_2, \ldots, A_N$. Authority A*i* manages a set of attributes $\tilde{A}_i = \{a_i,1, a_i,2, \ldots, a_i, n_i\}$ and specifies an (k_i, n_i)-threshold access structure A_i, for $i = 1, 2, \ldots, N$. Ai generates a secret-public key pair $((\alpha_i, \beta_i), (Y_i, Z_i))$ and publishes (Y_i, Z_i). For each attribute $a_{ij} \in \tilde{A}_i$, A_i creates a secret-public key pair $(t_{i,j}, T_{i,j})$ and publishes $T_{i,j}$. The secret keys and public keys of A_i are $(\alpha_i, \beta_i \{t_{i,j}\}_{ai,j \in \tilde{A}i})$ and $(Y_i, Z_i, \{T_{i,j}\}_{ai,j \in \tilde{A}i})$, respectively. To issue secret keys to *a* user *U* with a set of attributes A_U, the authority A_i selects a random number r_i $\xleftarrow{R}$ Z_p and computes D_i using r_i, his secret key (α_i, β_i) and the user's identifier *u*. Hence, the user's identifier *u* is tied to his secret keys.

V. System Architecture

Architecture diagram shows the relationship between different components of system. This diagram is very important to understand the overall concept of system. Architecture diagram is a diagram of a system, in which the principal parts or functions are represented by blocks connected by lines that show the relationships of the blocks. They are heavily used in the engineering world in hardware design, electronic design, software design, and process flow diagrams.

In the above diagram contains user1, authority, user2, and database. First authority will be starting and user1 is running and then user2. Now user1 wants to send a message to user2. So user1 encrypt the message send it to authority with destination key, so authority will identify that key and sent is to user2. User2 will receive that message and he wants to decrypt that message. So user2 and authority will generate one private key it will be used to decrypt that message.
The systems architect provides the architects view of the users' vision.

VI. Performance Analysis

After designing any method it is necessary to test its performance which gives idea about working and the standards of its output. Performance analysis is looking at program execution to point out where bottleneck or other Performance problems might occur. Experimental and statistical analysis is carried out, to analyse the performance of the system.

For proposed system performance analysis is carried out with the help of some performance parameters used in Information security.

Where: $|u|$: Number of universal attributes.

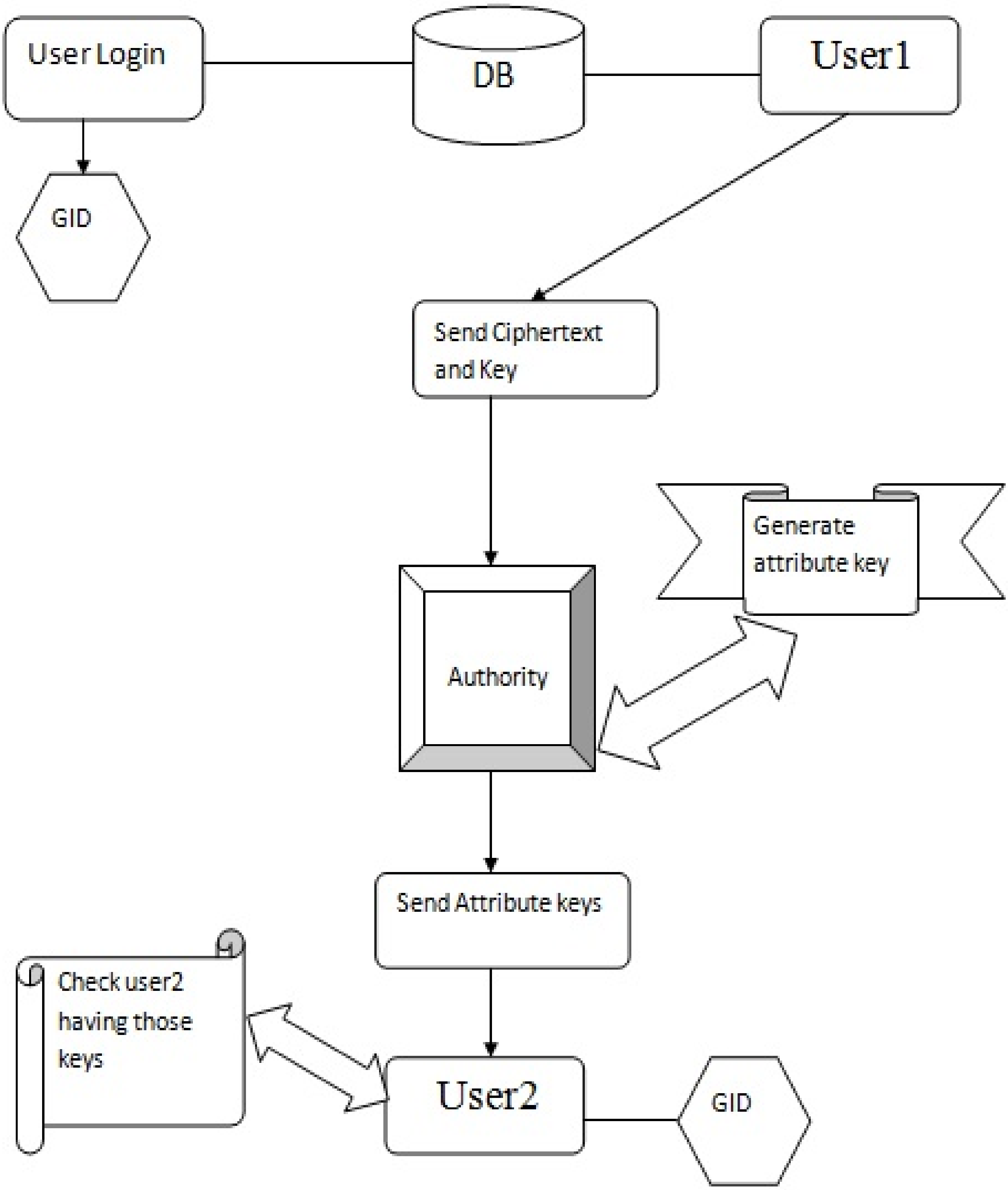

Fig : System Architecture

Parameters	**Chase's Scheme**	**Mullar Scheme**	**Chase & Chow Scheme**	**Lekwo& Water's Scheme**	**Liu Scheme**	**Proposed Scheme**
Computing Cost						
1. Authority Setup	$(\|u\|+1)E$	$2\|u\|E$	$(\|u\|+2N)E$	$2NE$	$(\|u+N\|E)$	$(\|u\|+2N)E$
2. KeyGen	$(I A_U\|+1)E$	$\|A_U\|E$	$(\|u\|+\|I_U\|^2)E$	$2\|A_U\|E$	$(4d+\|A_U\|)E+\|I_U\|P$	$(\|A_U\|+\|I_U\|+\|P_k\|)E$
3. Encryption	$(\|A_C\|+2)E$	$3\|I_C\|E$	$(\|A_C\|+2)E$	$(5\|A_C\|+1)E$	$(3\|A_C+2\|)E$	$(\|A_C\|+3)E$
4. Decryption	$\|A_C\|E+(\|A_C\|+1)P$	$2P$	$\|A_C\|E+(\|A_C\|+1)P$	$3\|A_C\|(E+P)$	$(\|A_C\|+1)E+2\|A_C\|P$	$\|A_C\|E+(\|A_C\|+\|I_C\|+1)P$
ABE Policy	Key policy	Ciphertext policy	Key policy	Ciphertext policy	Ciphertext policy	Key policy
Type of Authority	Single	Single	No	No	Multiple	No
Attribute Authority	No	No	No	No	Multiple	No
Security Model	Selective Set	Full Security	Selective Set	Full Security	Full Security	Selective Set
Length of Ciphertext	$(\|A_C\|+1)E_G+E_{Gr}$	$2\|I_C\|E_G+\|I_C\|E_{Er}$	$(\|A_C\|+1)E_G+E_{Gr}$	$2\|A_C\|E_G+(\|A_C\|+1)+E_{Gr}$	$(2\|A_C\|+1)E_G+E_{Gr}$	$(\|A_C\|+2)\ E_G+E_{Gr}$
Privacy preserved	No	No	Yes	No	No	Yes
Standard model	No	Yes	`No	Yes	Yes	Yes

E: One exponential operation.

N: Number of authorities in the system.

P: One pairing operation

$|A_c|$: Attribute required by ciphertext

$|A_U|$: Attribute held by user U.

$|I_C|$ and $|I_U|$: Index set of authorities such that A^i_U != {ϕ} and A^i_C != {ϕ}

A^i_U = the common attributes present among user and authority

A^i_C != the common attributes present among ciphertext and authority

E_G= One element in group G

E_{G_r} = One element in group G_r

P_K: Private key or session key

Above table shows performance analysis of proposed system on the basis of parameters like Computing cost , Attribute based Encryption policy, Type of Authority for monitoring system , Level of security , Length of ciphertext, Level of privacy, Length of secret key *etc.*[28]

1) Computing cost –
2) ABE (Attribute Based Encryption) policy
3) Type of Authority
4) Level of security
5) Length of ciphertext
6) Level of privacy
7) Standard model

1. Computing cost

Computing cost for attribute based encryption system can be calculated by considering various parameters such as

Authority setup, Key Generation, methods used for Encryption and Decryption.

Authority Setup - ABE (Attribute Based Encryption) Policy

In an open communication environment, such as Internet, sensitive data must be encrypted before being transmitted. To achieve this, encryption scheme can be employed to protect the confidentiality of the sensitive data. Traditional encryption schemes cannot express a complex access policy and additionally the sender must know all the public keys of the receivers. Attribute-based encryption (ABE) is a more efficient encryption scheme and express a complex acess structure. In an ABE scheme both the user's secret keys and the ciphertext are labeled with sets of attributes.

There are two kinds of ABE schemes:

1. Key-policy ABE (KP-ABE)

In these schemes, the secret keys are associated with an access structure while the ciphertext is labeled with set of attributes. Authority selects access structure to control who can decrypt the ciphertext.

2. Ciphertext-policy ABE (CP-ABE)

In these schemes, the ciphertext is associated with an access structure ,while the secret keys are labelled with set of attributes. Enryptor selects access structure to control who can decrypt the ciphertext. In proposed method, KP-ABE is used & access structure is selected by the authority to control who can decrypt the ciphertext.

A. Type Of Authority: There are two types of Authority: Single and Multiple.

Single Authority –

Only one authority is available which works as central authority (CA). The most challenging aspect of a single authority ABE scheme is collusion resistance. A single authority sees all the attributes requested by a user and gives a secret key and can easily re-randomize the secret sharing appropriately.

Multiple Authority

In multi-authority scheme, user must submit his GID (Global Identifier) to each authority to obtain corresponding secret keys. There are multiple authorities available and can be differentiated into two types

Centralized multiple authority

A Multi Authority ABE system is composed of K attribute authorities and one central authority.

De-centralized multiple authorities

A Multi Authority ABE system is composed of multiple authorities, which works in cooperation with each other. There is no central authority. In proposed system, multiple authorities can work independently without any cooperation and central authority. Any authority can join or leave system freely without the need of re-initializing the system.

Level of Security

There are two types of security models. One is Full security model and another is selective set security model. In proposed method, selective set security model is used. Privacy Preserving Decentralized ABE Π = (Global Setup, Authority Setup, BlindKeyGen, Encryption, Decryption) is secure in the selective set model under DBDH assumption.

Length of Ciphertext

The length of ciphertext is mainly depend on attribute required for ciphertext, the elements present in cyclic group, and randomization.

Level of Privacy

In decentralized ABE, privacy is preserved because here there is no use of global identifier using which authority can trace users. Here we have used private session key in order to improve privacy.

Standard Model

Proposed system uses DBDH as a standard model for ABE Advantages:

1. It is decentralized version of KPABE plus CPABE. In proposed method access specifier is decided by key so it uses KPABE concept. And the decryption of ciphertext is described by client/ user and not the authority so it is CPABE.
2. The key generation process is somewhat simplified. Involvement of authority is limited.
3. Security is improved with the help of session key.

VII. Conclusion

This paper proposed the Privacy-preserving decentralized key-policy ABE scheme, from this we can give the privacy to each and every authorities to take own decision. Malicious authorities cannot get user's attributes and secret keys because authorities not having any cooperation between them and no need to submit his GID to authorities.

References

[1] sze-ming.chow *"New Privacy-Preserving Architectures for Identity-Attribute-based Encryption"*

[2] N. P. Smart, "Access control using pairing based cryptography," in *The Cryptographers' Track at the RSA Conference - CT-RSA'03*, vol. 2612 of *LNCS*, pp. 111–121, 2003.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings: IEEE Symposium on Security and Privacy (S & P'07)*, (Oakland, California, USA), pp. 321– 34, IEEE, May 20-23 2007.

[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proceedings: Advances in Cryptology - EUROCRYPT'05* (R. Cramer, ed.), vol. 3494 of *Lecture Notes in Computer Science*, (Aarhus, Denmark), pp. 457–473, Springer, May 22-26 2005.

[5] M. Chase, "Multi-authority attribute based encryption," in *Proceedings: Theory of Cryptography Conference-TCC'07* (S. P. Vadhan, ed.), vol. 4392 of *Lecture Notes in Computer Science*, (Amsterdam, The Netherlands), pp. 515–534, Springer, February 21-24 2007.

[6] A. Lewko and B. Waters, "Decentralizing attribute - based encryption," in *Proceedings: Advances in Cryptology-EUROCRYPT'11* (K. G. Paterson, ed.), vol. 6632 of *Lecture Notes in Computer Science*, (Tallinn, Estonia), pp. 568–588, Springer, May 15-19 2011.

[7] J. Li, Q. Huang, X. Chen, S. S. M. Chow, D. S. Wong, and D. Xie, "Multi-authority ciphertext-policy attribute-based encryption with accountability," in *Proceedings: ACM Symposium on Information, Computer and Communications Security-ASIACCS'11*, pp. 386–390, ACM, 2011.

[8] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Proceedings: Advances in Cryptology-CRYPTO'01* (J. Kilian, ed.), vol. 2139 of *Lecture Notes in Computer Science*, (Santa Barbara, California, USA), pp. 213–229, Springer, August 19-23 2001.

[9] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings: Advances in Cryptology - CRYPTO'84* (G. R. Blakley and D. Chaum, eds.), vol. 196 of *Lecture Notes in Computer Science*, (Santa Barbara, California, USA), pp. 47–53, Springer, August 19-22 1985.

[10] C. Gentry, "Practical identity-based encryption without random oracles," in *Proceedings: Advances in Cryptology-EUROCRYPT'06* (S. Vaudenay, ed.), vol. 4004 of *Lecture Notes in Computer Science*, (St. Petersburg, Russia), pp. 445–464, Springer, May 28-June 1 2006.

[11] B. Waters, "Efficient identity-based encryption without random oracles," in *Proceedings: Advances in Cryptology-EUROCRYPT'05* (R. Cramer, ed.), vol. 3494 of *Lecture Notes in Computer Science*, (Aarhus, Denmark), pp. 114–127, Springer, May 22-26 2005.

[12] D. Boneh and X. Boyen, "Efficient selective-id secure identitybased encryption without random oracles," in *Proceedings: Advances in Cryptology-EUROCRYP'04* (C. Cachin and J. Camenisch, eds.), vol. 3027 of *Lecture Notes in Computer Science*, (Interlaken, Switzerland), pp. 223–238, Springer, May 2-6 2004.

[13] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *Proceedings: ACM Conference on Computer and Communications Security-CCS'09* (E. Al- Shaer, S. Jha, and A. D. Keromytis, eds.), (Chicago, Illinois, USA),pp. 121–130, ACM, November 9-13 2009.

[14] L. Cheung and C. Newport, "Provably secure ciphertext policy abe," in *Proceedings: ACM Conference on Computer and Communications Security - CCS'07* (P. Ning, S. D. C. di Vimercati, and P. F. Syverson, eds.), (Alexandria, Virginia, USA), pp. 456–465, ACM, October 28-31 2007.

[15] J. Herranz, F. Laguillaumie, and C. R´afols, "Constant size ciphertexts in threshold attribute-based encryption," in *Proceedings: Public Key Cryptography-PKC'10* (P. Q. Nguyen and D. Pointcheval, eds.), Lecture Notes in Computer Science, (Paris, France), pp. 19– 34, Springer, May 26-28 2010.

[16] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters,"Fully secure functional encryption: Attribute- based encryption and (hierarchical) inner product encryption," in *Proceedings: Advances in Cryptology-EUROCRYPT'10* (H. Gilbert:, ed.), vol. 6110 of *Lecture Notes in Computer Science*, (French Riviera), pp. 62–91, Springer, May 30 - June 3 2010.

[17] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive,efficient, and provably secure realization," in *Proceedings: Public Key Cryptography - PKC'11* (D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, eds.), vol. 6571 of *Lecture Notes in Computer Science*, (Taormina, Italy), pp. 53–70, Springer, March 6-9 2011.

[18] A. Beimel, *Secure Schemes for Secret Sharing and Key Distribution*. Phd thesis, Israel Institute of Technology, Technion, Haifa, Israel, June 1996.

[19] N. Attrapadung and H. Imai, "Dual-policy attribute based encryption," in *Proceedings: Applied Cryptography and Network Security-ACNS'09* (M. Abdalla, D. Pointcheval, P.-A. Fouque, and D. Vergnaud, eds.), vol. 5536 of *Lecture Notes in Computer Science*, (Paris-Rocquencourt, France), pp. 168–185, Springer, June 2-5 2009.

[20] A. Rial and B. Preneel, "Blind attribute-based encryption and oblivious transfer with fine-grained access control," in *2010th Benelux Workshop on Information and System Security-WISSec'10*, pp. 1–20, 2010.

[21] M. Naor, B. Pinkas, and O. Reingold, "Distributed pseudo - random functions and KDCs," in *Proceedings: Advances in Cryptology - EUROCRYPT'99* (J. Stern, ed.), vol. 1592 of *Lecture Notes in Computer Science*, (Prague, Czech Republic), pp. 327–346, Springer, May 2-6 1999.

[22] Z. Liu, Z. Cao, Q. Huang, D. S. Wong, and T. H. Yuen, "Fully securemulti-authority ciphertext-policy attribute-based encryption without random oracles," in *Proceeedings: European Symposium on Research in Computer Security-ESORICS'11* (V. Atluri and C. Diaz, eds.), vol. 6879 of *Lecture Notes in Computer Scienc*, (Leuven, Belgium), p. 278297, Springer, September 12-14 2011.

[23] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," in *Proceedings: Advances in Cryptology- CRYPTO'97* (B. S. K. Jr., ed.), vol. 1294 of *Lecture Notes in Computer Science*, (Santa Barbara, California, USA), pp. 410–424, Springer, August 17-21 1997.

[24] J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy, "Blind and anonymous identity-based encryption and authorised private searches on public key encrypted data," in *Proceedings: Public Key Cryptography - PKC'09* (S. Jarecki and G. Tsudik, eds.), vol. 5443 of *Lecture Notes in Computer Scienc*, (Irvine, CA, USA), pp. 196–214, Springer, March 18-20 2009.

[25] M. Green and S. Hohenberger, "Blind identity-based encryption and simulatable oblivious transfer," in *Proceedings: Advances in Cryptology-ASIACRYPT'07* (K. Kurosawa, ed.), vol. 4833 of *Lecture Notes in Computer Science*, (Kuching, Malaysia), pp. 265–282, Springer, December 2-6 2007.

[26] D. Chaum, "Security without identification: Transaction systems to make big brother obsolete," *Communication of ACM*, vol. 28, no. 10, pp. 1030–1044, 1985.

[27] J. Camenisch and A. Lysyanskaya, "An efficient system for nontransferable anonymous credentials with optional anonymity revocation," in *Proceedings: Advances in Cryptology-EUROCRYPT'01* (B. Pfitzmann, ed.), vol. 2045 of *Lecture Notes in Computer Scienc*, (Innsbruck, Austria), pp. 93–118, May 6-10 2001.

[28] Han J., Susilo W., Mu Y., and Yan J., "Privacy-preserving decentralized key-policy attribute-based encryption ," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 11, pp. 2150-2162, 2012