Efficient and Secure Data in Disruption Tolerant Network Using Attribute Based Encryption

G.Mallika¹, Dr.P.Kuppusamy²
¹ PG Student, Department of Computer Science and Engineering, Gnanamani College of Technology, Namakkal
² Professor, Department of Computer Science and Engineering, Gnanamani College of Technology, Namakkal

ABSTRACT
Attribute-based encryption (ABE) is a new cryptographic primitive which provides a promising tool for addressing the problem of secure and fine-grained data sharing and decentralized access control. Key-policy attribute-based encryption (KP-ABE) is an important session of ABE, where cipher texts are categorized with sets of attributes and private keys are associated with access structures that control which cipher texts a user is competent to decrypt. KP-ABE has mainuses in data sharing on untrusted cloud storage. In previous multi-authority key-policy attribute-based Encryption (KP-ABE) schemes, both a super control central authority subsists, or multiple attribute establishments must collaborate in modifying the system. In this paper, we propose a new fully secure decentralized KP-ABE scheme, where no central authority exists and there is no cooperation between any multiple attribute authorities. To become an AA, a participant needs to create and publish its unrestricted factors. All the user's private keys will be connected with his unique global identifier (GID). The efficiency of our scheme is almost as well as that of the underlying fully secure single-authority KP-ABE system. In our scheme, we can revoke one attribute of a user instead of all attributes issued to him and the user can complete decryption as long as the unrevoked attributes of the user satisfy the access ecreation. The revocation does not disturb any other user's private key. Additionally, our system supports an important thing for succeeding the user accountability to prevent illegal key sharing among colluding users.

Index Terms-Attribute based encryption (ABE), Central authority, Decentralized access control, Global identifier, Key Policy Attribute based encryption(KP-ABE).

1. INTRODUCTION
The concept of attribute-based encryption (ABE) which was proposed by Sahai and Waters[1] has attracted much attention in research in recent years. There are two complementary forms of ABE: key policy attribute based encryption(KP-ABE)[2] and ciphertext policy attribute based encryption(CPABE).
In CP-ABE systems [3], [4], [5], [6], [7], such situation is inverse. i.e., the ciphertext is annotated with an access policy, while the user’s private key is annotated with some attributes.Senders can encrypt a message with a specific access policy in terms of access structure over attributes, stating what kind of receivers will be able to decrypt the ciphertext. Users have set of attributes and achieve corresponding secret attribute keys from the attribute ability. Such a consumer can decrypt a ciphertext if his/her attribute satisfies the access policy associated to the ciphertext.
In the ABE systems aforementioned, there is only one authority which issues and manages the universe of attributes. These single-authority ABE schemes are not applicable while the attributes may be issued by different authorities. To address this issue, Chase [8] proposed the first multiauthority KP-ABE system. Chase [8] also presented an approach to resist collusion attacks in multi-authority settings. In her scheme, there are a central authority (CA) and multiple attribute authorities (AAs). Each user is given a unique global identifier (GID). All the user’s attribute-related keys requested from different AAs must be linked with his GID. Additionally, the CA will issue GID-related key to the user. Since CA knows all of the AAs’ secret keys, it can decrypt every ciphertext. For the first time, ABE enables public key based one-to-many encryption. However, two important problems must be considered when applying ABE schemes to practical applications. The first problem is revocation mechanism which is necessary for any ABE schemes involving many users. And the second problem is user accountability which prevents illegal key sharing among colluding users. For the revocation scheme of ABE, Pirretti et al.[9] proposed the first key revocation scheme. Later, Boldyreva et al.[10] proposed a revocable ABE scheme extended from their revocable IBE. Both of the two schemes require the users to periodically go to the authority for key reissuing. Based on the previous work mentioned above,

www.ijaert.org
Attrapadung et al. [11] defined two revocation models explicitly: indirect revocation model which enforces revocation by the key authority who releases a key update material periodically; the other is direct revocation model which enforces revocation directly by the sender who specifies the revocation list while encrypting. Attrapadung et al. [11] also proposed a new cryptosystem called Broadcast ABE which supports direct identity revocation mechanism. We note that, in the ABE schemes mentioned above, the revocation of user identity would revoke the entire user access privilege and the revocation of attributes would affect others who share the same attributes. For the user accountability of ABE, Hinek et al. proposed the first scheme which resolved the key abuse problem of users. But in their scheme, another third party should be involved in each user’s decryption which makes it impractical. Use the technique of identity-based encryption with wildcards to achieve the accountability of users. Li et al. [12] and Yu et al. [13] also proposed ABE schemes which achieve the user accountability.

2. RELATED WORK

CP-ABE is more suitable to DTNs than KP-ABE because it supports encryptors such as a commanderto select an access policy on attributes and to encrypt privatedata under the access egression via encrypting with theconsistent public keys or attributes [14], [15], [16].

2.1 Attribute Revocation: Bethencourt et al. [17] and Boldyreva et al. [10] first submitted key revocation toolsin CP-ABE and KP-ABE, correspondingly. Their results are attached to each attribute asfinishing data and allocates new set of keys to effective users after the expiration. Theinsert attribute revocable ABE schemes have two main complications. The first problem is the security degradation in relations of the backward and forward secrecy. It is an extensive scenario that users such as warriors may change their attributes repeatedly, e.g., position or place move when seeing theseas attributes. Then, a user who recently holds the attribute might be able to enter the previous data encrypted previously heobtains the attribute until the data is reencrypted with the recently updated attribute keys by periodic rekeying.

The second problem is scalability. The key authority sometimes announces a key update factually by unicast at each time-slot so that all of the nonrevoked users can inform theirkeys. This results in the “1-affects-” problem, which means that the update of a particular attribute affects the entire nonrevoked users who share the attribute. This could be a blockage for both the key authority and all nonrevoked users. The direct key revocation can be done by retracting usersusings ABE that supports negative sections. To do so, one just improves conjunctively the AND of negation of retracted user identities. However, this solution still slightly lacks efficiency performance. This scheme will stand overhead group elements additively to the scope of the ciphertext and multiplicatively to the size of private key over the new CP-ABE scheme of Bethencourt et al. [16], where is the extremesize of revoked attributes set. Golle et al. also planned a user revocable KP-ABE scheme, but their system only works when the amount of attributes associated with a ciphertext is accurately half of the universe size.

2.2 Key Escrow: Most of the existing ABE structures are constructed on the construction where a single trusted authority hasthe control to generate the whole private keys of users with its major secret information. Thus, the key escrow problem is essential such that the key expert can decrypt every ciphertext addressed to users in the scheme by creating their secret keys at any stage. A distributed KP-ABE scheme that solves the key escrow problem in a multiauthority system. In this methodology, all attribute authorities are sharing in the key generation protocol in a circulated way such that they cannot group their data and link many attribute sets belong to the similar user. One disadvantage of this fully distributed method is the recital degradation. Since there is no integrated authority with master secret data, all attribute authorities should connect with each other in the system to produce a user’s secret key.

2.3 Decentralized ABE: Distributed CP-ABE schemes in the multiauthority network location. They achieved a collective access policy over the attributes distributed from different authorities by basically encrypting data multiple times. The main disadvantages of this method are efficiency and expressiveness of access procedure. Chase proposed multiauthority KP-ABE and CP-ABE methods, respectively. However, their patterns also smart from the key escrow problem similar the prior decentralized patterns.

3. PRELIMINARIES

3.1 Bilinear Pairing

Let G1, G2, GT be multiplicative groups of prime order p. The elements g1 ∈ G1 and g2 ∈ G2 are producers of G1
and G2 separately. A bilinear pairing is a map $e : G1 \times G2 \rightarrow GT$ with the following things:

3.1.1. Bilinear: $e(g1a; g2b) = e(g1; g2)ab$ for all $g1 \in G1, g2 \in G2$, where $a, b \in \mathbb{Z}_p$.

3.1.2. Non-degenerate: There exists $g1 \in G1$ and $g2 \in G2$ such that $e(g1; g2) \neq 1$; in other words, the map does not show all pairs in $G1 \times G2$ to the identity in $GT$.

3.1.3. Computability: There is an effective algorithm to calculate $(g1; g2)$ for all $g1 \in G1$ and $g2 \in G2$.

### 3.2 Access Structure

3.2.1. Access Structure: Let $P = \{P1, P2, \ldots, Pr\}$ represent a set of events. A collection $A = \{P1, P2, \ldots, PT\}$ is monotonic if $\forall A1, A2$: if $A1 \subseteq A$ and $A1 \subseteq A2$ then we have $A2 \subseteq A$. An admission structure (correspondingly, monotone access building) is a group (respectively, monotone collection) $A$ of non-empty subgroups of $P$. That is, $A \subseteq \{P1, P2, \ldots, PT\} \setminus \emptyset$. We say that the sets in $A$ are the eligible sets, and the sets external $A$ are the criminal sets.

Among ABE systems, the part of the parties is exchanged by the expressive attributes. In this way, the legal set of attributes will be controlled in the access structure $A$. We emphasis on the monotonic access structure in this paper. To understand common access structures, one can basically consider the denial of an attribute as a distinct attribute.

### 4. METHODOLOGY

#### 4.1 Ciphertext Policy Attribute-Based Encryption (CP-ABE):

In a cipher procedure attribute-based encryption scheme [11], each user’s key is linked with a set of attributes demonstrating their abilities, and a ciphertext is encoded.

#### 4.2 RC4:

RC4 is a stream code, symmetric key algorithm. The similar algorithm is used for both encryption and decryption as the files stream is simply XORed with the produced key sequence. The key stream is totally independent of the plaintext recycled. It uses a variable size key from 1 to 256 bit to set a 256-bit state counter. The state table is used for succeeding generation of pseudo-random bits and then to create a pseudo-random stream which is XORed with the plaintext to provide the ciphertext.

This algorithm creates a stream of pseudo-random values. The input stream is XORed with these standards, bit by bit. The encryption and decryption procedure is the same as the data stream is just XORed with the prepared key order. If it is worked in unarranged message, it will crop the decrypted message production, and if it is served in plaintext message, it will create the coded form [6]. The RC4 encryption process is shown in Fig.1.

![Fig.1.RC4 Encryption Algorithm](image-url)

#### 4.3 Key Policy Attribute based Encryption (KP_ABE):

4.3.1 Syntax of KP_ABE

Let $U = \{attr1, \ldots, attrn\}$ be the creation of possible attributes, where each attribute represents an attribute and $n$ is the total quantity of attributes. A KP-ABE system is parameterized by a universe of probable attributes $U$, and contains of the following four polynomial-time processes.

Setup($\lambda, U$): The setup algorithm proceeds as input these security limitations $\lambda$ and the attribute universe $U$. It outputs some civic parameters $\text{params}$ and the major secret key $msk$. The trusted attribute authority (AA) issues $\text{params}$ and keeps $msk$ secret.

KeyGen($\text{params}, msk, A$): The key generation process takes as input the public criticisms $\text{params}$, the
master clandestine key $msk$ and an contact organization A which his allocated by the AA to the user. It outputs a decryptionkey $SKA$ related with the access structure $A$.

Encrypt$(params, W, m)$: The encryption algorithm proceeds as input the public parameters $params$, a set of qualities $W$ and a message $m \in \{0, 1\}^*$. It outputs the ciphertext $c$.

Decrypt$(params, c, SKA)$: The decryption system takes as input the public limitations $params$, the ciphertext $c$ that was encrypted under the set of qualities $W$, and the decryption key $SKA$ for access structure $A$. It outputs the message $m$ if $W \in A$.

In a KP-ABE scheme, ciphertexts are related to aset of attributes $W$ and private keys related to accessstructures $A$. Decryption is probable when the attribute set $W$ is approved in the access structure $A$, i.e., $W \in A$.

**Definition:** A KP-ABE scheme is correct if for any$(params, msk) \leftarrow$ Setup$(1, \lambda, U)$, any sets of qualities $W \subseteq U$, any dispatch $m \in \{0, 1\}^*$, and any $SKA \leftarrow$ KeyGen$(params, msk, A)$ with $W \in A$, we have $\text{Decrypt}(params, \text{Encrypt}(params, W, m), SKA) = m$, with probability 1 over the unpredictability of all the algorithms.

The appearance was made active to securely achieve the data distributed in the data allocation system. Attribute collection keys are selectively distributed to the legal users in each attribute set, which then are used to re-encrypt the cipher text encoded under the CP-ABE and KP-ABE algorithm.

**REFERENCES**


5. CONCLUSION