**Improving Privacy and Security in Decentralized Cipher text Policy Attribute-Based Encryption**

**Abstract:**

In previous privacy-preserving multi-authority attribute-based encryption (PPMA-ABE) schemes, a user can acquire secret keys from multiple authorities with them knowing his/her attributes and furthermore, a central authority is required. Notably, a user’s identity information can be extracted from his/her some sensitive attributes. Hence, existing cannot fully protect users’ privacy as multiple authorities can collaborate to identify a user by collecting and analyzing his attributes. Moreover, cipher text-policy ABE (CPABE)is a more efficient public-key encryption where the encryptor can select flexible access structures to encrypt messages. Therefore, a challenging and important work is to construct a PPMA-ABE scheme where there is no necessity of having the central authority and furthermore, both the identifiers and the attributes can be protected to be known by the authorities. In this paper, a privacy-preserving decentralized CP-ABE (PPDCPABE)is proposed to reduce the trust on the central authority and protect users’ privacy. In our PPDCP-ABE scheme, each authority can work independently without any collaboration to initial the system and issue secret keys to users. Further more ,a user can obtain secret keys from multiple authorities with out them knowing anything about his global identifier (GID) and attributes.

**Existing System:**

Most existing public key encryption methods allow a party to encrypt data to a particular user, but are unable to efficiently handle more expressive types of encrypted access control.Existing PPMAABE schemes cannot fully protect users’ privacy as multiple authorities can collaborate to identify a user by collecting and analyzing his attributes. Moreover, ciphertext-policy ABE (CPABE) is a more efficient public-key encryption where the encryptor can select flexible access structures to encrypt messages. Therefore, a challenging and important work is to construct a PPMA-ABE scheme where there is no necessity of having the central authority and furthermore, both the identifiers and the attributes can be protected to be known by the authorities. In this paper, a privacy-preserving decentralized CP-ABE (PPDCPABE) is proposed to reduce the trust on the central authority and protect users’ privacy. In our PPDCP-ABE scheme, each authority can work independently without any collaboration to initial the system and issue secret keys to users. Furthermore, a user can obtain secret keys from multiple authorities without them knowing anything about his global identifier (GID) and attributes.

**Proposed System**:

We proposed a privacy-preserving decentralized ABE scheme to protect the user’s privacy. In our scheme, all the user’s secret keys are tied to his identifier to resist the collusion attacks while the multiple authorities cannot know anything about the user’s identifier. Notably, each authority can join or leave the system freely without the need of reinitializing the system and there is no central authority. Furthermore, any access structure can be expressed in our scheme using the access tree technique. Finally, our scheme relies on the standard complexity assumption, rather than the non-standard complexity assumptions. proposed a MACP-ABE scheme with accountability. In this scheme, the anonymous key issuing protocol was employed. Specifically, a user can be identified when he shared his secret keys with others. Likewise, the multiple authorities must cooperate to initialize the system. Recently, a privacy-preserving decentralized KP-ABE (PPDKP-ABE) scheme was proposed In this scheme, multiple authorities can work independently without any collaboration. Especially, a user can obtain secret keys from multiple authorities without releasing anything about his GID to them, and the central authority is not required. proposed a privacy-preserving decentralized CPABE (PPDCP-ABE) scheme where simple access structures can be implemented. Nevertheless, similar to that in , the authorities in these schemes can also collect the user’s attributes.

**Scope:**

Future research direction regarding PPDCP-ABE, it would be interesting to construct a fully secure PPDCP-ABE scheme since the scheme proposed in this paper is selectively secure.

**Problem Statement:**

**Challenges**:

* When constructing a PPDCP-ABE scheme, the following technical hurdles must be overcome.
* First, the collusion attacks must be resisted. Since the DCPABE scheme was constructed in the radome oracle model, the collusion attacks can be easily resisted by tieing the user’s secret keys to his GID.
* However, it is challenging to resist the collusion attacks in the DCP-ABE scheme which is designed in the standard model;
* Second, the user must convince each authority that the attributes for which he is obtaining secret keys are monitored by the authority as the authority cannot know his attributes;
* Third, the authority can interact with the user to generate correct secret keys for him even if he dose not know the user’s identifer and attributes; Finally, the secret keys derived from multiple authorities can be used together to decrypt a cipher text. Techniques.
* To overcome the hurdles mentioned above, the following techniques are exploited. In , to resist the collusion attacks, each authority Ai ties a user’s secret keys to his GID by computing H(GID)yi where yi is Ai’s secret key and H(·) is a hash function.
* In the standard model, when creating secret keys for a user, each authority selects a random number t and computes gtg β+μ t where g is the generator of a group G, β is the partial master secret key of the authority and μ is the user’s identifier. Therefore, the secret keys generated for different users cannot be combined.
* For the second problem, we exploit the set-membership proof technique. For each attribute, the authority specifies an un forgeable authentication tag such that a user can prove in zero knowledge that the attribute for which he is possessing a secret key is monitored by the authority.
* To resolve the third problem, we use the idea in the CPABE scheme [9] and 2-party secure computing technique.
* In the traditional ABE schemes, for each attribute, the authority selects a secret key r and publishes the corresponding public key gr.

**IMPLEMENTATION**

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it’s constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

**MODULE DESCRIPTION**:

1. **Attribute-based Encryption**
2. **Cryptography**
3. **Encryption And Decryption**
4. **Decentralization**
5. **Privacy.**

**Attribute Based Encryption**

**Global Setup(1\_)** → params. This algorithm takes as input a security parameter \_ and outputs the system parameters params.

**Authority Setup(1\_)** → (SKi, PKi,Ai). Each authority Ai generates his secret-public key pair KG(1)\_ → (SKi, PKi) and an access structure Ai, for i = 1, 2, ・ ・ ・ ,N.

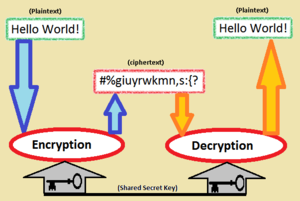
**KeyGen(SKi,GID,Ai GID)** → SKiU. Each authorityAi takes as input his secret key SKi, a global identifierGID and a set of attributes AiGID, and outputsthe secret keys SKiU, where AiGID = AGID\_A˜i,AGID and A˜i denote the attributes correspondingto the GID and monitored by Ai, respectively

**Encryption (params,M,AC)** → CT. This algorithm takes as input the system parameters params, a message M and a set of attributes AC, and outputs the ciphertext CT, where AC = {A1 C,A2 C, ・ ・ ・ ,ANC } and Ai C = AC\_A˜i.

**Decryption(GID, {SKiU}i∈IC, CT).** This algorithm takes as input the global identifier GID, the secret keys {SKiU}i∈IC and the ciphertext CT, and outputs the message M, where IC is the index set of the authorities Ai such that Ai C \_= {φ}.

**Cryptography**

The art of protecting information by transforming it ([*encrypting*](http://www.webopedia.com/TERM/E/encryption.htm) it) into an unreadable format, called [cipher text](http://www.webopedia.com/TERM/C/cipher_text.htm). Only those who possess a secret *key* can decipher (or [*decrypt*](http://www.webopedia.com/TERM/D/decryption.htm)) the message into [plain text](http://www.webopedia.com/TERM/P/plain_text.htm). Encrypted messages can sometimes be broken by cryptanalysis, also called *code breaking*, although modern cryptography techniques are virtually unbreakable.

****

**Encryption and Decryption**

**Encryption**

In an encryption scheme, the message or information (referred to as [plaintext](http://en.wikipedia.org/wiki/Plaintext)) is encrypted using an encryption algorithm, turning it into an unreadable [cipher text](http://en.wikipedia.org/wiki/Ciphertext) (ibid.). This is usually done with the use of an [encryption key](http://en.wikipedia.org/wiki/Key_%28cryptography%29), which specifies how the message is to be encoded. Any adversary that can see the cipher text, should not be able to determine anything about the original message.

**Decryption**:

An authorized party, however, is able to decode the ciphertext using a decryption algorithm, that usually requires a [secret decryption key](http://en.wikipedia.org/wiki/Key_%28cryptography%29), that adversaries do not have access to. For technical reasons, an encryption scheme usually needs a key-generation algorithm, to randomly produce keys.

**Decentralization**:

The term "decentralization" embraces a variety of concepts which must be carefully analyzed in any particular country before determining if projects or programs should support reorganization of financial, administrative, or service delivery systems. Decentralization -- the transfer of authority and responsibility for public functions from the central government to intermediate and local governments or quasi-independent government organizations and/or the private sector -- is a complex multifaceted concept. Different types of decentralization should be distinguished because they have different characteristics, policy implications, and conditions for success.

**Privacy**: Privacy is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively. The boundaries and content of what is considered private differ among cultures and individuals, but share common themes. When something is private to a person, it usually means that something is inherently special or sensitive to them. The domain of privacy partially overlaps security, which can include the concepts of appropriate use, as well as protection of information. Privacy may also take the form of bodily integrity. The right not to be subjected to unsanctioned invasion of privacy by the government, corporations or individuals is part of many countries' privacy laws, and in some cases, constitutions. Almost all countries have laws which in some way limit privacy. An example of this would be law concerning taxation, which normally require the sharing of information about personal income or earnings. In some countries individual privacy may conflict with freedom of speech laws and some laws may require public disclosure of information which would be considered private in other countries and cultures.

**Algorithm**:

Commitment Schemes.

A commitment scheme consists of the following three algorithms.

* Setup(1κ) → params. Taking as input a security parameter 1κ, this algorithm outputs the public parameters params.
* Commit(params,m) → (com, decom). Taking as input the public parameters params and a message m, this algorithm outputs a commitment com and a decommitment decom
* . decom can be used to decommit com to m. Decommit(params, m, com, decom) → {0, 1}.
* Taking as input the public parameters params, the message m, the commitment com and the decommitment0 decom, this algorithm outputs 1 if decom can decommit com to m; otherwise, it outputs 0.
* A commitment scheme must exhibit two properties: hiding and binding. The hiding property requires that the message m keeps unreleased until the user releases it later, while the binding property requires that only the value decom can be used to decommit the commitment com to m.

**H/W System Configuration:-**

**Processor - Pentium –III**

Speed - 1.1 GHz

RAM - 256 MB (min)

Hard Disk - 20 GB

Floppy Drive - 1.44 MB

Key Board - Standard Windows Keyboard

Mouse - Two or Three Button Mouse

Monitor - SVGA

**S/W System Configuration:-**

Operating System : Windows95/98/2000/XP

Application Server : Tomcat5.0/6.X

Front End : HTML, Java, Jsp

Scripts : JavaScript.

Server side Script : Java Server Pages.

Database : My sql

Database Connectivity : JDBC.

**Conclusion**:

Some PPMA-ABE schemes have been proposed to protect users’ privacy and reduce the trust on the central authority. Nevertheless, only the privacy of the GID was considered in the existing scheme. Since sensitive attributes can also reveal the users’ identities, existing schemes cannot provide a full solution to protect users’ privacy in MA-ABE schemes. In this paper, we proposed a PPDCP-ABE scheme where both the privacy of the GID and the attributes are concerned. In our scheme, a central authority is not required and multiple authorities can work independently without any cooperation. A user can convince the authorities that the attributes for which he is obtaining secret keys are monitored by them without showing the attributes to them. Therefore, our scheme provides a perfect solution for the privacy issues in MA-ABE schemes. As for future research direction regarding PPDCP-ABE, it would be interesting to construct a fully secure PPDCP-ABE scheme since the scheme proposed in this paper is selectively secure.