CONTROL CLOUD DATA ACCESS PRIVILEGE AND ANONYMITY WITH FULLY ANONYMOUS ATTRIBUTE-BASED ENCRYPTION

ABSTRACT

 Cloud computing is a revolutionary computing paradigm, which enables flexible, on-demand, and low-cost usage of computing resources, but the data is outsourced to some cloud servers, and various privacy concerns emerge from it. Various schemes based on the attribute-based encryption have been proposed to secure the cloud storage. However, most work focuses on the data contents privacy and the access control, while less attention is paid to the privilege control and the identity privacy. In this paper, we present a semianonymous privilege control scheme AnonyControl to address not only the data privacy, but also the user identity privacy in existing access control schemes. AnonyControl decentralizes the central authority to limit the identity leakage and thus achieves semianonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. Subsequently, we present the AnonyControl-F, which fully prevents the identity leakage and achieve the full anonymity. Our security analysis shows that both AnonyControl and AnonyControl-F are secure under the decisional bilinear Diffie–Hellman assumption, and our performance evaluation exhibits the feasibility of our schemes.

EXISTING SYSTEM

 we present a semianonymous privilege control scheme AnonyControl to address not only the data privacy, but also the user identity privacy in existing access control schemes.

Besides the fact that we can express arbitrarily general encryption policy, our system also tolerates the compromise attack towards attributes authorities, which is not covered in many existing works.

We extend existing schemes by generalizing the access tree to a privilege tree.

we extend existing schemes by generalizing the access tree to a privilege tree.

 The key point of the identity information leakage we had in our previous scheme as well as every existing attribute based encryption schemes is that key generator issues attribute key based on the reported attribute, and the generator has to know the user’s attribute to do so.

**PROPOSE SYSTEM**

Various schemes based on the attribute-based encryption have been proposed to secure the cloud storage.

 Various techniques have been proposed to protect the data contents privacy via access control.

we propose AnonyControl and AnonyControl-F (Fig. 1) to allow cloud servers to control users’ access privileges without knowing their identity information.

They will follow our proposed protocol in general, but try to find out as much information as possible individually.

The proposed schemes are able to protect user’s privacy against each single authority. Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F.

We firstly implement the real toolkit of a multiauthority based encryption scheme AnonyControl and AnonyControl-F.

# SYSTEM CONFIGURATION

**SOFTWARE REQUIREMENTS**:

 Operating System : Windows

 Technology : Java and J2EE

 Web Technologies : Html, JavaScript, CSS

 IDE : My Eclipse

 Web Server : Tomcat

 Tool kit : Android Phone

 Database : My SQL

 Java Version : J2SDK1.5

**HARDWARE REQUIREMENTS**:

 Hardware : Pentium

 Speed : 1.1 GHz

 RAM : 1GB

 Hard Disk : 20 GB

 Floppy Drive : 1.44 MB

 Key Board : Standard Windows Keyboard

 Mouse : Two or Three Button Mouse

 Monitor : SVGA

### 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:**

# Number of Modules

After careful analysis the system has been identified to have the following modules:

1. **Registration based Social Authentication Module**
2. **Security Module**
3. **Attribute-based encryption module.**
4. **Multi-authority module.**
5. **Registration -Based Social Authentication Module:**

The system prepares trustees for a user Alice in this phase. Specifically, Alice is first authenticated with her main authenticator (i.e., password),and then a few(e.g., 5) friends, who also have accounts in the system, are selected by either Alice herself or the service provider from Alice’s friend list and are appointed as Alice’s Registration.

1. **Security Module:**

Authentication is essential for securing your account and preventing spoofed messages from damaging your online reputation. Imagine a phishing email being sent from your mail because someone had forged your information. Angry recipients and spam complaints resulting from it become your mess to clean up, in order to repair your reputation. trustee-based social authentication systems ask users to select their own trustees without any constraint. In our experiments (i.e., Section VII), we show that the service provider can constrain trustee selections via imposing that no users are selected as trustees by too many other users, which can achieve better security guarantees

**3.Attribute-based encryption module.**

Attribute-based encryption moduleis using foreach and every node encrypt data store. After encrypted data and again the re-encrypted the same data is using for fine-grain concept using user data uploaded. the attribute-based encryption have been proposed to secure the cloud storage. Attribute-Based Encryption (ABE). In such encryption scheme, an identity is viewed as a set of descriptive attributes, and decryption is possible if a decrypter’s identity has some overlaps with the one specified in the ciphertext.

**4.Multi-authority module.**

A multi-authority system is presented in which each user has an id and they can interact with each key generator (authority) using different pseudonyms. Our goal is to achieve a multi-authority CP-ABE which achieves the security defined above; guarantees the confidentiality of Data Consumers’ identity information; and tolerates compromise attacks on the authorities or the collusion attacks by the authorities. This is the first implementation of a multi-authority attribute based encryption scheme.