A Pre-Authentication Approach to Proxy Re-encryption in Big Data Context

ABSTRACT

Big data is a hot research topic. More and more users prefer to save their data in the cloud center because the cloud has a considerable amount of storage space, and users can download their data anywhere and anytime. People take photos, record music and do many other operations on their personal equipments, producing large amount of data. As a matter of fact, the demand of cloud storage space is growing faster than ever before. When people upload their data to the cloud, the first thing they may confider is whether the cloud storage is secure or not. They do not want other persons to peep their data without their permission. Public key encryption is a mechanism designed for data providers to encrypt their data, and thus protecting the privacy of their data. Except the data receivers who have valid private key, no one can access the data. For example, in a hospital system, the patient records are too large and hard to store. A solution is to upload the massive data to the cloud for storage. Since everyone has access to the cloud, the data needs to be encrypted to prevent the private information of patients from being leaked out. When doctors intend to access the records, they decrypt the ciphertext by using their keys and obtain the message they need.

EXISTING SYSTEM

In Existing system Public Key Encryption (PKE), the privacy required by the patients could be ensured. Up to now, many cryptographic encryptions methods have been proposed to satisfy the requirements of privacy- preserving in big data storage. However, most encryption methods such as the public key encryption are not anonymous, i.e., if the adversaries obtain the ciphertexts, they can easily know the owner of the ciphertext as well as who will receive the ciphertext. The PKE cannot achieve the anonymity of the users send and receive the ciphertext, so personal information may be leaked. If an adversary is able to achieve the ciphertext, he can know whose key the ciphertext is encrypted under, thus knowing the owner of the ciphertext.

DRAWBACKS

- Encryption methods such as the public key encryption are not anonymous.
- The adversaries obtain the ciphertexts, they can easily know the owner of the ciphertext as well as who will receive the ciphertext.

PROPOSED SYSTEM

This paper proposes the notion of pre-authentication for the first time, i.e., only users with certain attributes that have already. The pre-authentication mechanism combines the advantages of proxy conditional re-encryption multi-sharing mechanism with the attribute-based authentication technique, thus achieving attributes authentication before re-encryption, and ensuring the security of the attributes and data. Moreover, this paper finally proves that the system is secure and the proposed pre-authentication mechanism could significantly enhance the system security level.

ADVANTAGES

- The pre-authentication mechanism combines the advantages of proxy conditional re-encryption multi-sharing mechanism with the attribute-based authentication technique.
- Achieving attributes authentication before re-encryption, and ensuring the security of the attributes and data.

SYSTEM REQUIREMENTS

- **H/W System Configuration:-**
- Processor - Pentium –IV
- RAM - 4 GB (min)
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

- **S/W System Configuration:-**
- Operating System : Windows 7 or 8 32 bit
- Application Server : Tomcat5.0/6.X
- Backend coding : Java
- Tool : Virtual Box

- Environment : Ubuntu
- Technology : Hadoop