Privacy-Preserving Ciphertext Multi-Sharing Control for Big Data Storage

Abstract

The need of secure big data storage service is more desirable than ever to date. The basic requirement of the service is to guarantee the confidentiality of the data. However, the anonymity of the service clients, one of the most essential aspects of privacy, should be considered simultaneously. Moreover, the service also should provide practical and fine-grained encrypted data sharing such that a data owner is allowed to share a ciphertext of data among others under some specified conditions. This project, for the first time, proposes a privacy-preserving ciphertext multi-sharing mechanism to achieve the above properties. It combines the merits of proxy re-encryption with anonymous technique in which a ciphertext can be securely and conditionally shared multiple times without leaking both the knowledge of underlying message and the identity information of ciphertext
senders/recipients. Furthermore, this paper shows that the new primitive is secure against chosen-ciphertext attacks in the standard model.

EXISTING SYSTEM
Cryptographic encryption mechanisms can be employed to fulfill the requirement. For instance, Public Key Encryption (PKE) allows a data sender to encrypt the data under the public key of receiver such that no one except the valid recipient can gain access to the data.

DRAWBACK OF EXISTING SYSTEM
- Data owner has to be on-line all the time.
- Decryption and re-encryption is time consumed and computation costly.
- Suffers from a limitation
- Trusted third party with knowledge of the decryption key of the data owner may be delegated to handle the task.
PROPOSED SYSTEM

It combines the merits of proxy re-encryption with anonymous technique in which a ciphertext can be securely and conditionally. New primitive is secure against chosen-ciphertext attacks in the standard model. Proxy Re-Encryption (PRE) is proposed to tackle the dilemma of data sharing

Identity-Based Proxy Re-Encryption (IBPRE), which offers a practical solution for access control in networked file storage

ADVANTAGE OF PROPOSED SYSTEM

➢ “on-line all the time” requirement is unnecessary.
➢ Knowledge shared multiple times without leaking.
SYSTEM SPECIFICATION

Hardware Requirements

- System : Pentium IV 2.4 GHz
- Hard Disk : 40 GB
- Floppy Drive : 1.44 Mb
- Monitor : 15 VGA Colour
- Mouse : Logitech
- Ram : 512 Mb

Software Requirements

- Operating system : Windows Family
- Tools : eclipse/Netbeans
- Technology Used : Java
- Backend Used : SQL Server