Cost-Effective Authentic and Anonymous Data Sharing with Forward Security

Abstract

Data sharing has never been easier with the advances of cloud computing, and an accurate analysis on the shared data provides an array of benefits to both the society and individuals. Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. Ring signature is a promising candidate to construct an anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purpose. Yet the costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. Identity-based (ID-based) ring signature, which eliminates the process of certificate verification, can be used instead. In this paper, we further enhance the security of ID-based ring signature by providing forward security: If a secret key of any user has been compromised, all previous generated signatures that include this user still remain valid. This property is especially important to any large scale data sharing system, as it is impossible to ask all data owners to re-authenticate their data even if a secret key of one single user has been compromised. We provide a concrete and efficient instantiation of our scheme, prove its security and provide an implementation to show its practicality.
**EXISTING SYSTEM**

An accurate analysis on the shared data provides an array of benefits to both the society and individuals. Data sharing with a large number of participants must
take into account several issues including efficiency, data integrity and privacy of data owner.

**DRAWBACK OF EXISTING SYSTEM**

- Service is provided at an acceptable level even under network attacks.
- Access control only eligible users can have the access to the data.

**PROPOSED SYSTEM**

Ring signature is construct an anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purpose.

**ADVANTAGE OF PROPOSED SYSTEM**

- Ring signature by providing forward security.
- Smart Grid can obtain their personal energy usage data with others one can compare their energy consumption with others it ability to access, analyze.

**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