Fuzzy Identity-Based Data Integrity Auditing for Reliable Cloud Storage Systems

ABSTRACT

- As a core security issue in reliable cloud storage, data integrity has received much attention. Data auditing protocols enable a verifier to efficiently check the integrity of the outsourced data without downloading the data.
- A key research challenge associated with existing designs of data auditing protocols is the complexity in key management.
- In this paper, we seek to address the complex key management challenge in cloud data integrity checking by introducing fuzzy identity-based auditing- the first in such an approach, to the best of our knowledge.

- More specifically, we present the primitive of fuzzy identity-based data auditing, where a user's identity can be viewed as a set of descriptive attributes. We formalize the system model and the security model for this new primitive. We then present a concrete construction of fuzzy identity-based auditing protocol by utilizing biometrics as the fuzzy identity. The new protocol offers the property of error-tolerance, namely, it binds private key to one identity which can be used to verify the correctness of a response generated with another identity, if and only if both identities are sufficiently close.

EXISTING SYSTEM

- Despite the benefits offered by cloud storage, there are many inherent security risks since when data owners out-source their data to the cloud, they generally lose physical possession of their data and even have no idea where their data are actually stored or who has the permission to getting access to their data.
- That is to say, it is the cloud servers who control the fate of the data after the data owners uploading their files to the cloud. The cloud servers assure they will try their best to protect the security of the cloud data, but the data loss accidents are inevitable.

- This is not surprising. Firstly, a short-time crash of the cloud server or the breakdown of the storage medium(e.g RAM) will cause the data easily corrupted. Moreover, users' data may be lost due to deliberate deletion by cloud servers in order to make the available storage space for other files to get more profit. Data loss incident happens frequently in reality and has been regarded as one of the key security concerns in cloud storage.

DISADVANTAGES

- Data auditing protocols is the complexity in key management.
- Security issue in reliable cloud storage

PROPOSED SYSTEM

- 1)We propose the notion of fuzzy identity-based data integrity auditing designed to simplify key management.
- 2) We then formalize the system model and security model to ensure the security called soundness of this new primitive (i.e. if a cloud server can convince a verifier that the server is storing a file, if and only if it is actually storing that file).
- 3) We describe a concrete construction of fuzzy identity-based data integrity auditing protocol, by borrowing the idea of fuzzy identity-based encryption due to Shacham and Waters.

ADVANTAGES

- Reduces the burden of maintenance and management of the data.
- Best to protect the security of the cloud data, but the data loss accidents are inevitable

HARDWARE AND SOFTWARE REQUIREMENTS

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 XP/7.
- Coding Language : ASP.net, C#.net /java

CONCLUSION

- Cloud storage services have become an increasingly important part of the information technology industry in recent years. ;
- With more users getting involved in cloud storage, ensuring the integrity of data outsourced to the cloud is of paramount importance. In this paper, we presented the first fuzzy identity-based data integrity auditing protocol.
- The proposed protocol revolutionizes key management in traditional remote data integrity checking protocols.

- We also presented the the system and security models for this primitive, and a concrete fuzzy identity-based data integrity auditing protocol using the biometric-based identity as an input. We then demonstrated the security of the protocol in the selective-ID model. The prototype implementation of the protocol demonstrates the practicality of the proposal