Fine-Grained Access Control for Cloud Data

Description

Users outsource encrypted data to cloud to achieve data confidentiality and help users retain control over the outsourced cloud data. Encryption of cloud data should fulfil the usual practice of fine-grained access control while providing flexible user revocation support.

This technology enables users’ decryption capabilities on the need-to-know basis, coupled with cloud-assisted user revocation at virtually no cost. In particular, the data owner will deposit a proxy key for each authorized user at the cloud, which is used for “proxy decryption”, a function helping partially decrypt encrypted data. The proxy keys indelibly involve the cloud’s private key, which can reduce trust upon the cloud. User revocation is achieved by simply deleting the revoked user’s proxy key instructed by the data owner. The system is featured as client efficient, such that user decryption is lightweight thus users can also use resource-constrained devices (e.g., mobile phone, tablet) to access encrypted cloud data.

Features

- Fine-grained data sharing
- Immediate and efficient user revocation
- Lightweight user decryption
- Reduced trust upon cloud

Applications

- Healthcare
- Finance
- Data-Critical Cloud Applications

References

- “Methods for Providing Requested Data from a Storage Device to a Data Consumer and Storage Devices”. US patent pending (US20140052985).

Department of Infocomm Security, Institute for Infocomm Research (http://icsd.i2r.a-star.edu.sg)
1 Fusionopolis Way, #21-01 Connexis (South Tower), Singapore 138632
Contact: Eunice Pee (IDM) Tel: (65) 64082180 Email: eunice-pee@i2r.a-star.edu.sg