論文の内容の要旨

Thesis Summary

Achieving Expressive, Scalable, and Efficiently Revocable Collaborative Data Access Control in Multi-Authority Cloud

(マルチオーソリティクラウドにおけるデータアクセス制御の表現性、スケーラビリティ、効率的な失効処理の実現)

ファクキアウ ソムチャート　　Somchart Fugkeaw

(本文 Body)

Cryptographic-based access control is a palpable solution for supporting flexible and secure data access control in data outsourcing environment. However, dealing with both access control enforcement and complexity of cryptographic keys is non-trivial. Among the models employed, Ciphertext Policy- Attribute-based Encryption (CP-ABE) is regarded as a suitable solution and mostly adopted since it reduces key management overhead compared to symmetric and public key encryption. In addition, CP-ABE provides the owners with the full control over their own policies. Nevertheless, there are no works that apply CP-ABE and show the practicality in implementing it in the complex and collaborative data sharing scenario where multiple users in different domains can access the data shared by multiple owners. Furthermore, the major drawbacks of CP-ABE related to the inability to express and enforce write privilege, the high communication and computation costs of key distribution, revocation, and policy updates are still re-current problems that have not been solved in an integrated manner by any previous works.

In this thesis, we propose an expressive, scalable, and efficiently revocable access control solution supporting collaborative data sharing in multi-authority cloud storage systems. Furthermore, all drawbacks of CP-ABE mentioned above are resolved in this thesis based on the following four key technical contributions.

First, we propose the access control scheme called Collaborative Ciphertext-Policy Attribute Role Based Encryption (C-CP-ARBE) based on the combination of Role-based Access Control (RBAC) and a Ciphertext-Policy Attribute-based Encryption (CP-ABE). We adopt a RBAC model to enhance the expressiveness of CP-ABE policy. At a conceptual level, the access control

policy is designed to accommodate the privilege information that comprehensively expresses read and write access of each user. In addition, we propose a write access enforcement mechanism to enable write-permitted users to update data and retrieve the policy to re-encrypt it securely and efficiently.

Second, we propose the zero key broadcast encryption technique based on our proposed user decryption key graph and public key encryption for supporting efficient key management and minimizing key distribution cost. The proposed technique enables all generated keys to be securely stored in a cloud server and dynamically invoked upon the user`s request. Compared to the CP-ABE, our scheme provides more scalable and practical in supporting a large number of users.

Third, within the cryptographic process of C-CP-ARBE, we propose a two-layer encryption (2LE) scheme to enable a more efficient user revocation with the computation cost reduction for user key re-generation and file re-encryption. With our 2LE method, a data is encrypted with the CP-ABE and then the ciphertext is encrypted with the AES symmetric encryption. Our proposed scheme minimizes the cost of user revocation in a manner where there is no file re-encryption and key re-generation if there is a user revocation. Our strategy is to update symmetric key based on the re-computation of the public role parameter. Hence, only the symmetric encryption layer is changed while the inner CP-ABE encryption layer is not affected. In addition to the user revocation level, we also investigate the problems of attribute revocation which is a finer level in CP-ABE. Revoking an attribute (s) introduces unavoidable overheads including expensive overheads for key re-generation, data re-encryption, and key re-distribution. To this end, we embed our newly proposed scheme called Very Lightweight Proxy Re-Encryption (VL-PRE) scheme into the C-CP-ARBE. In VL-PRE, size of the re-encryption key is small and key updates method is used instead of key generation. These properties of VL-PRE significantly reduce the computation cost for computing the re-encryption key in all revocation cases.

Another core focus in this thesis is the proposal of an optimized and scalable policy update management scheme. In CP-ABE, the data owner needs to re-encrypt files and send them back to the cloud when the policy is updated. This incurs overheads including computation, communication, and maintenance cost at data owner side. To this end, we develop policy updating algorithms to handle the policy change and employ VL-PRE to optimize the cost of file re-encryption when there is an update of policy. The security proof and policy update validation

criteria are given to guarantee the security, correctness, and accountability of the proposed scheme.

To evaluate all the proposed features of C-CP-ARBE, we conducted the experiments by setting the simulations to evaluate the encryption, decryption, and revocation performance. Specifically, we did experiments to compare the performance of our C-CP-ARBE and related works regarding the user revocation, attribute revocation, and policy update performance. The experimental results confirm that our proposed C-CP-ARBE is practical and efficient in practice.