Securing Data with Provenance and Cryptography

アムリル, シャリム

出版情報：Kyushu University, 2018, 博士（情報科学）, 論文博士
バージョン：
権利関係：

（別紙様式２）

氏　　名　：Amril Syalim（アムリル　シャリム）

論文題名　：Securing Data with Provenance and Cryptography
（プロヴェナンスと暗号でのデータ安全性確保）

区　　分　：　甲　[✓ 乙]

論文内容の要旨

With the advances in the network technology, it is now possible to implement the databases and applications as services. The main advantage of this model is the users can use the services at a fraction of the cost to maintain their own servers. The users can also use a powerful distributed computational resource that is provided as a service for their computation heavy tasks. However, this model has a fundamental problem, because the data is stored in the servers owned by the entities that are not controlled by the users, the users need to concern about the confidentiality and integrity of their sensitive data.

In a distributed system, because the tasks can be executed by many computers, some auditors may need to verify the integrity of data produced by the system. Many researchers suggested the idea to implement the provenance concept in the distributed systems. In the context of the computer systems, the provenance of data is recorded as a collection of assertions created by the process executors that describe the origins and the processes to produce the data. The provenance is stored in a special database, we call the Provenance Store, that should be accessible to the auditors who need to verify the data integrity.

The Provenance Store should be protected from malicious entities who try to update the provenance assertions. The update to the provenance causes the integrity problems, namely “inconsistent claims” and “inconsistent interpretations” problems. Storing the provenance in a trusted storage can prevent the attack. However, it is not practical to be implemented in many systems. We propose an integrity scheme that can be used to detect any changes to the provenance assertions by employing a signature chain and assigning a consecutive counter produced by a Trusted Counter Server (TCS) to each assertion.

The provenance should also be protected from unauthorized accesses. The

existing methods for the access controls are designed for regular data that are not suitable for the provenance. A critical information in the provenance that needs to be protected by the access control is the causal relationships between the process and the data. We propose a method to implement access control system by defining the access right we call TRACE, that can be used to define access policy to a collection of assertions that have causal relationships to a specific assertion. We combine the TRACE right with a Multilabels method to support better granularity of the access restrictions.

In this thesis, we also discuss the method to protect the integrity of a sequence of documents by using digital signature. The signature is used to prove the authenticity of each document and the order of the documents in the sequence. The existing signature schemes have some disadvantages: either we need to include another information to prove the order of the sequence (i.e., trusted time-stamps/counters) or during the verification, we need to have access to all (or large numbers) of the signed documents. We propose a scheme that allows a party to sign a sequence of digital documents with the following characteristics: (1) the party can prove the order of the document in the sequence without having a trusted timestamps/counters, (2) the party can verify the authenticity of the members of the sequence without having access to all other members in the sequence, and (3) the storage that is needed for the signature is smaller than signing each member of the sequence.

To protect confidentiality of the data in an untrusted server, the data owner can encrypt the data before storing the data in the server. The problem is whenever the data owner needs to update the encryption key, the data owner needs to re-encrypt the data by downloading the data from the server, decrypting the data, encrypting the data with the new key and uploading the new encrypted data to the server. It is desirable to have more efficient re-encryption method where the data owner can securely delegate the re-encryption process to a semi-trusted party (i.e., a proxy). Most symmetric ciphers do not support proxy encryption because malleability (the ability to meaningfully convert the ciphertext) is not a desired property in a secure encryption scheme. We propose a symmetric encryption scheme that supports proxy re-encryption by first transforming the plaintext into a random sequence of blocks using a variant of an All or Nothing Transform (AONT), and then transforming the random sequences by using some combinations of permutations.

(734 words)