氏名	TRAN THAO PHUONG			
学位の種類	博士(情報科学)			
学位記番号	博情第 328 号			
学位授与年月日	平成 27 年 9 月 24 日			
論文題目	A STUDY ON SECURITY FOR CLOUD COMPUTING （クラウド・コンピューティングのセキュリティに関する研究）			
論文審査委員	主査	面 和成	北陸先端科学技術大学院大学	准教授
		宮地 充子	同	教授
		上原 隆平	同	教授
		緒方 和博	同	教授
		清本 晋作	KDDI 研究所	主任研究員

論文の内容の要旨

Since amount of data is increasing exponentially, data storage and management become burdensome tasks of the data owner. To reduce the burdens for the data owners, the concept of remote storage known as cloud has been proposed. A cloud is considered as a service through which the clients can use to publish, access, manage and share their data remotely and easily from anywhere via the Internet. Although data outsourcing reduces storage burden for the client, this method still has a problem that the service provider is typically not fully trusted. Thus, this model introduces numerous interesting research challenges: (i) data privacy, (ii) data availability and (iii) data integrity. Data confidentiality consists of the two research approaches: the cryptographic approach and the information-theoretic approach. In this study, we focus on integrity, availability and information-theoretic confidentiality. We choose the information-theoretic approach because our security analysis derives purely from information theory. Our goal is to construct a practical and secure cloud system. Based on this goal, we are interested in two research directions: Proof Of Retrievability (POR) and Secret Sharing Scheme (SSS).

The POR has been proposed to allow the client to check whether his/her data stored in the servers is available, intact and is always retrievable. Based on the POR protocol, four common techniques are used: replication, erasure coding, ORAM and network coding. In this study, we focus on the network coding because: it achieve better storage cost compared with replication, and better computation and communication costs compared with erasure coding and ORAM. Although many network coding-based PORs have been proposed, the efficiency and practicality have not been addressed simultaneously.

The SSS is a method for protecting distributed file systems against data leakage and data loss. In this scheme, the secret is encoded into a number of shares. The shares are then distributed among a group of participants where each participant holds a share of the secret. The secret can be only reconstructed when a sufficient number of shares are reconstituted. Although many SSSs are introduced, they have not achieved an optimal share size and have not supported the share repair feature.

In this dissertation, we propose three schemes, named the MD-POR (Multi-client and Direct repair for POR), DD-POR (Dynamic operation and Direct repair for POR) and SW-SSS (Slepian-Wolf coding-based SSS).

The MD-POR is our main proposed POR which has the following contributions: (i) The scheme can support direct repair feature. This means that if a corrupted server is detected, the healthy servers are required to provide their coded blocks directly to the new server. The new server can verify the provided coded blocks and can compute the new coded blocks for itself without disturbing the client. This mechanism can reduce the communication cost and the burden for the client; (ii) Multiple clients who own different secret keys can participant in the system. Their data are mixed together without losing the data confidentiality of individual clients; (iii) The scheme is constructed using symmetric key setting for the efficiency; and (iv) The scheme support public authentication. This means that not only the client but also any entity who has a given information can check the cloud servers while learning nothing about the secret key of each client. We employ a Third Party Auditor (TPA) on behalf of the clients to check the servers periodically. By delegating the responsibility of checking the servers to the TPA, the clients are free of the burden of checking the servers.

The DD-POR scheme is an improvement of the MD-POR scheme. Concretely, this scheme can support dynamic operations unlike the MD-POR scheme. The client not only can read the data but also can modify, insert, and delete the data. However, the DD-POR scheme is a partial improvement of the MD-POR scheme because in this DD-POR scheme, we can only deal with a single client instead of multiple clients as the MD-POR scheme. Furthermore, the DD-POR does not deal with the public authentication as the MD-POR scheme. The DD-POR scheme has the following contributions: (i) This scheme can support direct repair feature like the MD-POR scheme. When a server is corrupted, the healthy servers will provide their coded blocks and tags directly to the new server without sending them back to the client. Then, the new server can check them, and can compute the new coded blocks and the tags for itself; (ii) Unlike the MD-POR the client not only can check and retrieve the data, but also can perform dynamic operations such as modification, insertion and deletion on the data stored in the servers; and (iii) The scheme is constructed using symmetric key setting for the efficiency.

The SW-SSS scheme, we show that the Slepian-Wolf Coding, which is used to compress a data stream in a network, can be applied to the SSS to achieve the following advantages:(i) The shares are constructed using the XOR for fast computation; (ii) The parameter can be chosen arbitrarily; (iii) The direct share repair is supported; and (iv) The size of a share is optimized compared with

previous schemes.

Keywords: cloud computing, proofs of retrievability, secret sharing scheme, network coding, Slepian-Wolf coding.

論文審査の結果の要旨

クラウドサーバのデータが紛失して保存されていたデータの復旧が不可能になるという事故が実際に起きている．そのため，たとえクラウドサーバが信頼できないとしてもユーザのデータが守られる安全な仕組みが重要である．本論文は，可用性・完全性・機密性の観点から，クラウドストレージにおけるデータの安全性を高めるアルゴリズムに関する研究である．特に，ネットワーク符号を応用し，暗号学的にデータの復旧可能性を証明できる手法である POR（Proof of Retrievability）に主に焦点をあてている．

POR とは，クラウドサーバが信頼出来ないということを想定し，分散された複数のクラウドに預けられているデータが改ざんや欠落が無い本物のデータであり，かつ復旧可能であることをデータ所有者に保証するセキュリティプロトコルである. POR は, 単なる複製，消失符号，ネットワーク符号の大きく 3 つのデータ保存形式で使われることが想定されるが，本提案方式は効率性及びセキュリティの観点から最も優れているネットワーク符号をベースとする．ネットワーク符号ベースの POR 方式はこれまでにいくつか提案されているが，実用的かつ効率的な 2 つの性質，すなわち direct repair 及び動的処理機能がまだ実現できていない．direct repair とはクラウドサーバがダウンした際に残りの正当なクラウドサーバから新たなクラウドサーバに対して直接的にデータを復旧できる性質であり，既存研究ではクライアントが符号化データを復号して新しいサーバ用に再符号化する必要があった．また，動的処理はクラウド上のデータの追加，挿入，削除といった動的な処理を意味するが，既存研究ではこれらが一部しか実現できていなかった．

本研究では，direct repair かつ動的処理が可能なネットワーク符号をベースとした効率的な新たな POR を提案する．本方式は，共通鍵暗号ベースで設計されているため非常に軽量であり，既存のどの方式よりも効率的であることを示している．さらに，クラウドサーバによるデータの汚染攻撃及び覗き見攻撃を想定し，それらに対して耐性を与えている．

以上, 本論文は, クラウドサーバに対して実用的かつ効率的な 2 つの性質, すなわち direct repair（世界で初めて実現）及び動的処理機能を実現する新しい手法を与え，その有効性を示しており，学術的に貢献するところが大きい．よって，博士（情報科学）の学位論文として十分価値あるものと認めた．