Cryptographic Techniques that Combine Data Protection and Ease of Utilization in the Cloud Computing Era

Hitoshi Fuji, Atsushi Fujioka, Tetsutaro Kobayashi, Koji Chida, Fumitaka Hoshino, Toshiyuki Miyazawa, and Koutarou Suzuki

Abstract

In this article, we introduce cryptographic techniques that protect data in the cloud computing era while being easy to use. Specifically, we describe secure computing technology—which can keep private information confidential while enabling anonymous statistical analysis—and intelligent encryption, a cloud-managed-key cryptographic scheme, and an authenticated key exchange technique that together can protect data in cloud storage and prevent the leakage of keys.

1. Introduction

In recent years, the quantity of data has been growing at an explosive rate, and the proportion of highly confidential data has also been increasing. According to one survey, the data generated or copied worldwide in 2010 amounted to 1.2 zettabytes (10^{21} bytes), of which 28% needed to be stored securely. This proportion is likely to increase in the future and is predicted to reach 33% by 2015 [1]. When critical data is stored and used in the cloud in such large quantities, we need technology to ensure that information is managed safely according to its degree of confidentiality and intended purpose and to ensure that it can be used safely (**Fig. 1**).

In this article, we introduce secure computing technology that can process confidential information, such as personal details and business records, and enable anonymous statistical analysis while ensuring that privacy is maintained; intelligent encryption and a cloud-managed-key cryptographic scheme that protect data used in the cloud and prevent information from being leaked; and an authenticated key exchange technique that can ensure confidential information is protected against leaks.

2. Technologies

2.1 Secure computing technology

With the changes in information processing platforms brought about by cloud computing, the management and practical application of confidential information is becoming more complex. One technique for protecting confidential information is secret sharing technology, which stores data in distributed form across multiple servers in such a way that safety is maintained even if data is leaked from any one of these servers [2]. NTT is researching and developing secure computing technology that can process shared secret information without restoring the original information. An outline of this processing technique is shown in **Fig. 2**.

A major feature of secure computing technology is that information processing is implemented cooperatively by multiple computers so that the data never exists intact on any one computer. This greatly

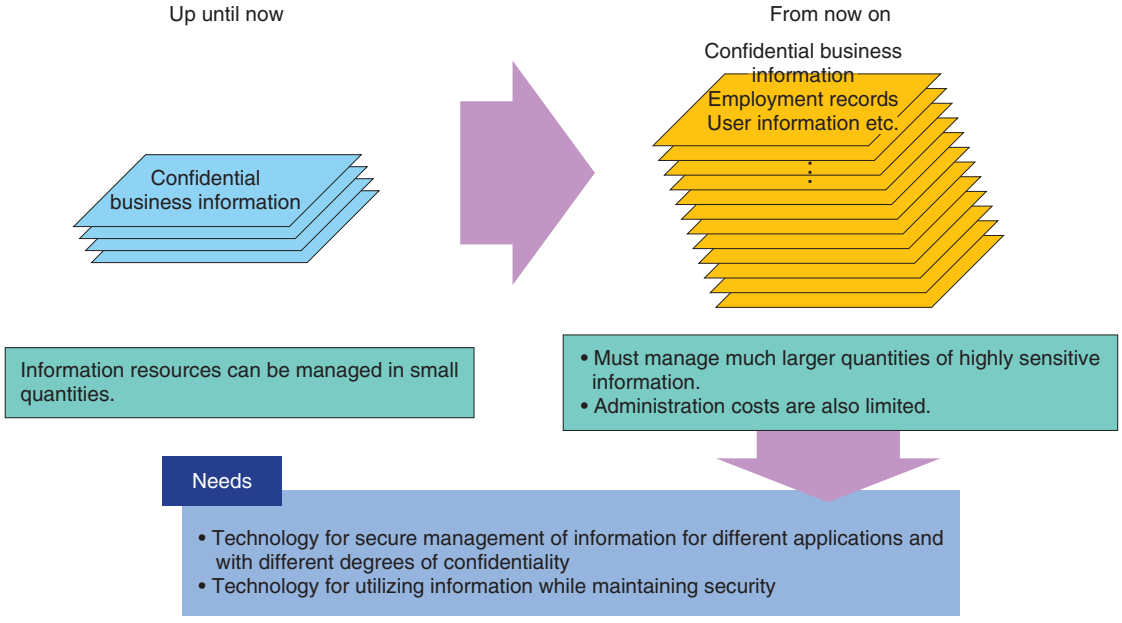

Fig. 1. Protecting information in the cloud computing era.

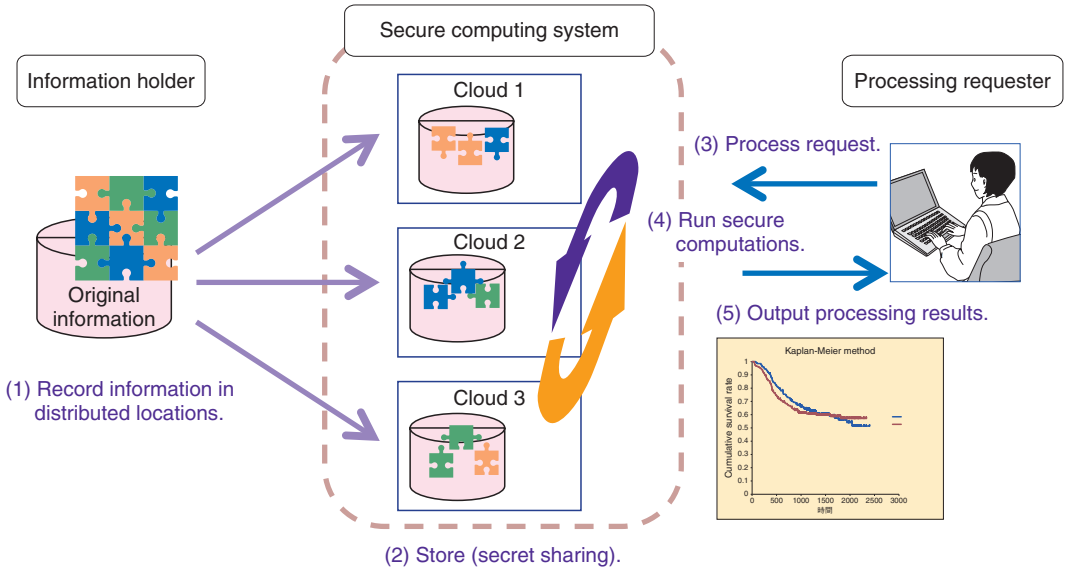

Fig. 2. Secure computing technology.

reduces the risk of information leaks and helps to dispel anxieties when information is provided to the cloud.

With the aim of facilitating the safe and secure utilization of clinical research data, the Japan Adult Leukemia Study Group and NTT were the first in the world to demonstrate the feasibility of secure computing technology in the processing of medical statistics, as announced in a press release in February 2012 [3], [4]. In this demonstration, we were able to output the results of medical statistics processing while maintaining the confidentiality of patient data

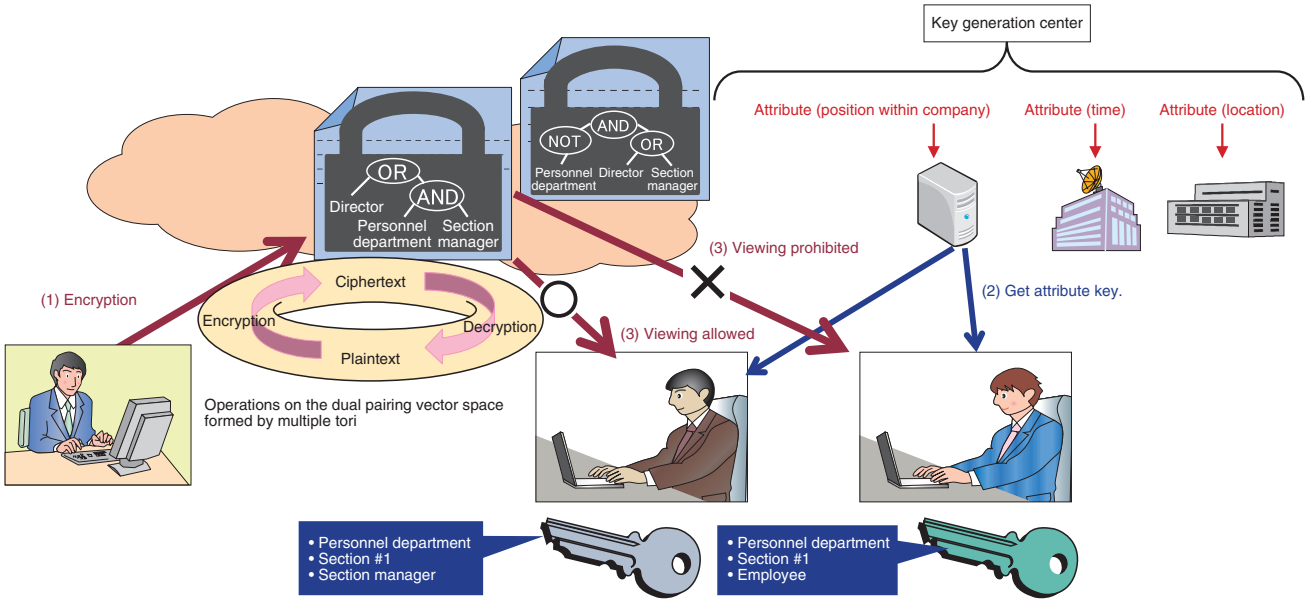

Fig. 3. Intelligent encryption.

registered from multiple medical facilities. This technology enables anonymous statistical analysis of confidential information held by various businesses.

Although secure computing technology is known to be secure in theory, its application to practical systems has been hindered by the limited processing speed. NTT's secure computing system is the fastest of its kind anywhere in the world: it has achieved a speed of 1 million multiplication operations per second as a basic performance indicator. By developing data manipulation operations based on our proprietary algorithms, we have made it possible to perform a wide variety of information processing tasks in a practical amount of time, such as sorting 10,000 records in two seconds while maintaining the confidentiality of the information being sorted. The demonstration of medical statistics processing was implemented with approximately 1000 data records, but we are working on improvements to our algorithms and hardware that will enable a diverse variety of information processing to be performed in a practical amount of time on large-scale data sets.

2.2 Intelligent encryption

Besides secret sharing, another method for protecting confidential information is the use of encryption, which has the advantage of allowing data to be stored safely at one location. However, conventional cryptography has required that only one person (the viewer) is authorized to see the clear content (plaintext) of the encrypted ciphertext. This makes it difficult for large numbers of people to access ciphertexts in the cloud. By contrast, intelligent encryption works by specifying, at the time of encryption, the conditions under which encrypted content can be viewed rather than the identity of the authorized viewer. This makes it possible to set up an access control system in which attribute keys corresponding to the attributes of each individual are distributed to viewers and viewing is allowed only when the viewing permission conditions and conditions related to the attribute keys held by the viewer (specified during encryption) have been met.

For example, consider the situation shown in **Fig. 3**, where access to confidential information is managed within a company. Conditions for viewing the information are incorporated into the ciphertext, and attribute information is applied to the decryption key so that decryption is possible only with a key that matches these conditions. If the data is encrypted with embedded conditions such as "[Director] OR [Personnel department AND Section manager]", then it can be decrypted with a key containing the attributes [Personnel department, Section #1, Section manager], but not by a key containing the attributes [Personnel department, Section #1, Employee].

We have also developed an improved version of intelligent encryption that supports multiple attribute

key creation stations [5]. With this method, keys corresponding to various attributes associated with a particular individual (department, time, location, address, age, etc.) are issued separately by organizations that are able to verify these attributes, thereby enabling control of this individual's access to encrypted files subject to usage conditions such as the department, time, or location, regardless of where these files are located.

Intelligent encryption is complete in terms of encryption theory, and we are currently working to develop peripheral technologies, such as communication protocols and key management methods, and to improve its processing performance.

With regard to communication protocols, conventional public-key and shared-key encryption systems rely on standard protocols and a pre-established public key certification infrastructure (public key infrastructure), allowing people all over the world to use encryption according to standard methods. We are working with universities and other research organizations with the aim of preparing standards and infrastructures to make intelligent encryption easily available to everyone.

With regard to the management of attribute keys, there are still issues specific to intelligent encryption that need to be resolved, such as the authentication of attribute information and the invalidation of compromised keys, and we are continuing to study ways of resolving these issues.

With regard to processing performance, we are currently at the level where it is possible to perform encryption and decryption in about 1 s on an ordinary personal computer. In the future, we aim to speed up the processing to the same level even on mobile devices, which are likely to become much more prevalent in the future.

2.3 Cloud-managed-key cryptographic scheme

An issue that affects all encryption techniques is the inherent danger of allowing users to manage (store and distribute) decryption keys themselves. Furthermore, since a user who has obtained a decryption key is then able to decrypt ciphertexts at any time, there is another problem in that users can still view the content of ciphertexts in situations where they no longer have the authority to do so.

NTT has therefore developed a cloud-managed-key cryptographic scheme (referred to hereinafter as the cloud cryptographic scheme) that solves the issue of key management in public key cryptography [6]. The cloud cryptographic scheme is a technique where decryption keys for public key cryptography are managed in the cloud (hereinafter referred to as a key management cloud), and the decryption processing is securely outsourced to the key management cloud. This allows users to make use of encrypted data without having to manage the decryption keys. Since the decryption processes can be enabled or disabled on the basis of authentication by the key management cloud, it is also possible to enable or disable the reading of a previously distributed ciphertext at a later time. This use of a key management cloud can provide a solution to the previous problem of needing a method for invalidating keys in intelligent encryption.

We are currently concluding our basic theoretical research on the cloud-managed-key cryptographic scheme, and we are also adding the final touches to a prototype system that can use highly confidential data in an online environment. To make this technology suitable for future business applications, we will press ahead with research aimed at practical applications and with the development of marketable systems. Specifically, we are continuing to investigate the availability of the key management cloud and the overall safety of the system, and we are conducting research and development aimed at specific services, such as applications to services that entrust data to the cloud (cloud storage services).

2.4 Authenticated key exchange

For secure exchange of information via public clouds or the Internet, there is a technique in which a secure communication channel is established by mutual authentication of two (or more) parties who want to exchange data by sharing keys used for confidential communication. This technique is called authenticated key exchange. An example of an authenticated key exchange scheme is SSL (Secure Socket Layer), which is upgraded whenever a vulnerability has been discovered.

As a result of its research on authenticated key exchange, NTT has developed an authenticated key exchange protocol [7] that satisfies the strongest level of safety and has been mathematically proven to be secure against all forms of key disclosure attack. An extended version of this protocol has been proposed to international standards organizations. In the above-mentioned intelligent encryption system, the person decrypting the information must have an attribute key for this purpose, but a technique for securely handing over attribute keys to the appropriate individuals in advance is also required. An authenticated key

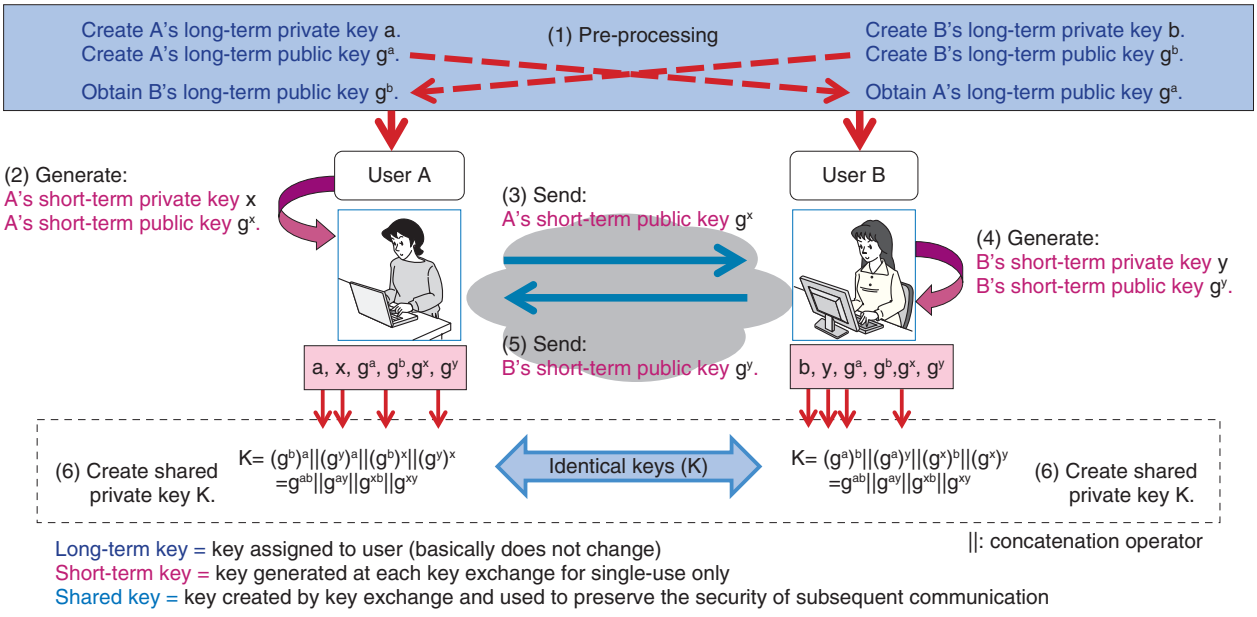

Fig. 4. Authenticated key exchange.

exchange can be used for this purpose.

An example of how authenticated key exchange is executed to share a shared key based on mutual authentication between two users over a public communication channel such as the Internet is shown in **Fig. 4**. Two users create shared keys as follows: each user performs exponential calculations based on his or her own long- and short-term private keys, called static and ephemeral keys, respectively, and the other user's long- and short-term public keys. The results are shared private keys that are guaranteed to be identical.

In this protocol, the long-term private keys are assigned to individual users and the short-term private keys are generated for each authenticated key exchange session. It is mathematically guaranteed that the confidentiality of the shared private keys is protected even if long-and short-term private keys are leaked in any combination (except in the case where both the long- and short-term private keys of the same user are compromised).

In addition to the public-key-based authenticated key exchange shown in Fig. 4, where authentication is performed between two users with public keys, there are also variants of authenticated key exchange such as a protocol where it is possible that a shared private key is shared only when the other party fulfills certain specified conditions, as in intelligent encryption. We are continuing to research these advanced authenticated key exchange protocols.

References

[1] J. Gantz and D. Reinsel, "Extracting Value from Chaos," IDC, 2011.
[2] K. Chida and K. Takahashi, "Privacy Preserving Computations without Public Key Cryptographic Operation," Proc. of the 3rd IWSEC (IWSEC 2008), Kagawa, Japan, Lecture Notes in Computer Science, Vol. 5312, pp. 184–200, 2008.
[3] Press release by NTT (in Japanese). http://www.ntt.co.jp/news2012/1202/120214a.html
[4] H. Shinohara, "R&D to Create the Future of ICT," NTT Technical Review, Vol. 10, No. 4, 2012. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201204fa2.html
[5] T. Okamoto and K. Takashima, "Efficient Attribute-based Signatures for Non-monotone Predicates in the Standard Model," Proc. of the 14th International Conference on Practice and Theory in Public Key Cryptography (PKC 2011), Taormina, Italy, Lecture Notes in Computer Science, Vol. 6571, pp. 35–52, 2011.
[6] G. Yamamoto and T. Kobayashi, "Self-correctors for Cryptographic Modules," Proc. of the 13th IMA International Conference on Cryptography and Coding (IMACC 2011), Oxford, UK, Lecture Notes in Computer Science, Vol. 7089, pp. 132–151, 2011.
[7] A. Fujioka and K. Suzuki, "Designing Efficient Authenticated Key Exchange Resilient to Leakage of Ephemeral Secret Keys", Proc. of the CT-RSA 2011, San Francisco, CA, USA, Lecture Notes in Computer Science, Vol. 6558, pp. 121–141, 2011.

Hitoshi Fuji
Senior Research Engineer, Supervisor, Information Security Project, NTT Secure Platform Laboratories.
He received the B.E. and M.E. degrees in industrial engineering from Tokyo University of Science in 1991 and 1993, respectively, and the Ph.D. degree in informatics. Since joining NTT in 1993, he has been engaged in research on software engineering, network security, and information security. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE).

Atsushi Fujioka
Senior Research Scientist, Supervisor, Information Security Project, NTT Secure Platform Laboratories.
He received the B.Eng., M.Eng., and D.Eng. degrees in electrical and electronic engineering from Tokyo Institute of Technology in 1985, 1987, and 1990, respectively. He joined NTT Communications and Information Processing Laboratories in 1990 and stayed at Swiss Federal Institute of Technology in Zurich, Switzerland, as an academic guest during 1993-1994. He is currently studying authenticated key exchange and identity-based identification. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is a member of IEICE.

Toshiyuki Miyazawa
Research Engineer, Planning Section, NTT Secure Platform Laboratories.
He received the B.E. and M.S. degrees in mathematics from Waseda University, Tokyo, in 2000 and 2003, respectively. Since joining NTT Information Sharing Platform Laboratory in 2003, he has been engaged in R&D of information security, especially of public key cryptography and security protocols. As a result of organizational changes in April 2012, he is now in NTT Secure Platform Laboratories. He is a member of the Japan Society for Industrial and Applied Mathematics. He received the SCIS (Symposium on Cryptography and Information Security) Paper Award from IEICE in 2007.

Tetsutaro Kobayashi
Senior Research Engineer, Information Security Project, NTT Secure Platform Laboratories.
He received the B.Eng. and M.Eng. degrees from Tokyo Institute of Technology in 1993 and 1995, respectively, and the Ph.D. degree from the University of Tokyo in 2005. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is currently engaged in research on information security. He received the SCIS (Symposium on Cryptography and Information Security) Paper Award in 2000.

Koutarou Suzuki
Senior Research Scientist, Information Security Project, NTT Secure Platform Laboratories.
He received the B.Sc., M.Sc., and Ph.D. degrees from the University of Tokyo in 1994, 1996, and 1999, respectively. Since joining NTT in 1999, he has been engaged in research on public key cryptography. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is a member of IEICE and IPSJ. He received the SCIS Paper Award in 2002.

Fumitaka Hoshino
Research Engineer, Information Security Project, NTT Secure Platform Laboratories.
He received the B.Eng. and M.Eng. degrees from the University of Tokyo in 1996 and 1998, respectively. He joined NTT in 1998. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories.

Koji Chida
Senior Research Engineer, Information Security Project, NTT Secure Platform Laboratories.
He received the B.S. and M.S. degrees in 1998 and 2000, respectively, and the Dr.Eng. degree in 2006, all from Waseda University, Tokyo. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is a member of IEICE and IPSJ. He received the IPSJ Best Paper Award in 2011.