NTT Press Releases

(News Release)

February 10, 2012

“Cloud-managed-key Cryptographic Scheme” as a Drastic Solution to Data Protection Issues in an Online Environment

- Safe Virtualization of the Cryptographic Process -

Nippon Telegraph and Telephone Corporation (NTT; Main Office: Chiyoda Ward, Tokyo; CEO: Satoshi Miura) has developed a cloud-managed-key cryptographic scheme (referred to below as “cloud cryptographic scheme”) to solve data protection issues in an online environment.
This is a new type of cryptographic scheme that manages the decryption keys (e.g. passwords, private keys, etc.) for unlocking encrypted data on the cloud. It is based on NTT’s new self-correction technique to achieve a new style of information sharing in an online environment.

1. Background

Services that pass private or highly confidential information to servers on the cloud or other online environments for further processing have begun to spread in recent years and are now becoming commonplace. This trend has been accompanied by new security issues as anxiety over data leaks and unauthorized use of data increase.
In response to this situation, a variety of encryption techniques have come to be tried to protect data and prevent information leaks, but in using existing encryption techniques, users themselves must perform prudent key management (for both storage and distribution). Users are also required to store and manage decryption keys on their own terminals or smart cards, which means that the occurrence of an accident during the course of key management increases the risk of information leaks.
In response to the above issues, NTT Information Sharing Platform Laboratories (referred to below as “NTT Laboratories”) has developed a new self-correction technique that can correct erroneous or bogus computations, and has used this technology to develop a cloud cryptographic scheme that can be used safely in an online environment. This system makes it easy for users to use a cipher and to prevent unauthorized use of encrypted data.

2. Mechanism and features of cloud encryption system

NTT’s cloud cryptographic scheme leaves and manages decryption keys on the cloud and safely consigns decryption of encrypted data to the cloud (**Figure 1**). This is achieved by software installed on the user’s terminal to interface with the cloud where the decryption keys are being managed so that encrypted data can be decrypted on the terminal.

(1) Safe and flexible management of decryption keys

In conventional encryption systems, a decryption key will be read into a user’s terminal to decrypt encrypted data. This approach, however, requires that all users manage decryption keys. NTT’s cloud cryptographic scheme, in contrast, manages decryption keys on the cloud itself without loading decryption keys into user terminals. The user is consequently released from management of decryption keys and is able to control the use of encrypted data in a simple and accurate manner.

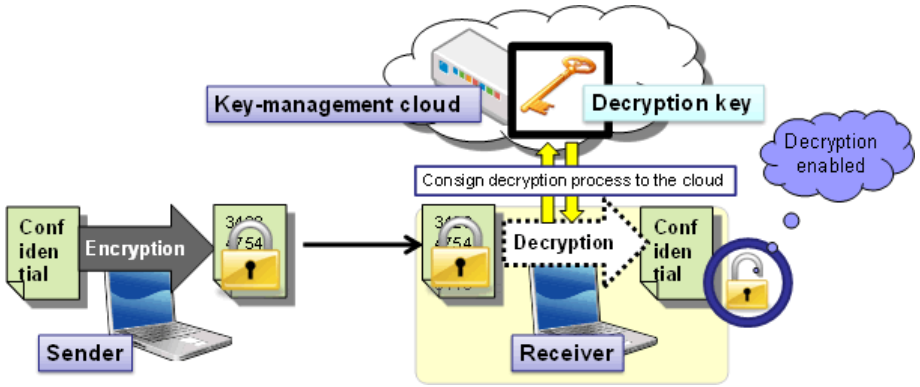

Figure 1: Mechanism of cloud encryption system

For example, this cloud cryptographic scheme enables a certain user to pass encrypted data to persons A, B, and C and to later make settings that allow only persons A and B to read that data and to then make another setting that prohibits person A from reading that data again (**Figure 2**). In other words, the scheme enables the creator of encrypted data to control who is to be allowed to decrypt that data so that the unauthorized use of data can be prevented even after the encrypted data has been distributed.

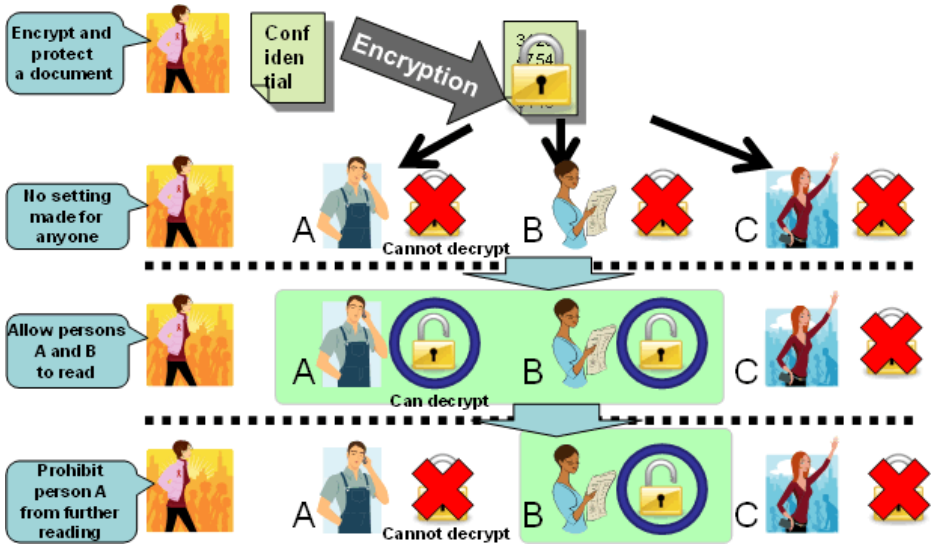

Figure 2: Safe and flexible use of encrypted data

(2) Self-correction technique that can correct any kind of error

The cloud cryptographic scheme was achieved by the background of a new self-correction technique developed by NTT Laboratories. When consigning the decryption of encrypted data to another computer, this technique extracts only correct computational results and ensures normal processing to be performed even if an error has occurred in the results of computations requested of that computer or if computational results have been disguised by a third person. This self-correction is achieved by requesting the other computer to perform computations several times and to then examine the results of those computations for consistency. At the same time, no information on the processing to be consigned to other computers is included in the data transferred.. In other words, the content of such processing is kept secret. In conventional technique, the ability of self-correction techniques to extract only correct computational results is limited depending on the properties or frequency of abnormalities such as errors and bogus data included in the computational results.

When requesting a computer to perform computations several times, this new self-correction technique (**Figure 3**) developed by NTT Laboratories can detect abnormalities by giving different sets of target data (Alternates 1 and 2 in the figure) a relationship that cannot be predicted by a third party. In effect, the technique extracts only correct computational results regardless of the types of abnormalities included in the target data enabling normal processing to be performed. In addition, the results of consigned processing such as decryption are even kept secret from the operator of the computer to which that processing was consigned. This technique therefore enables “virtualized cryptographic process” in which the decryption of encrypted data is consigned to the cloud while maintaining safety in an actual online environment. It also achieves a safe scheme for managing keys on the cloud.

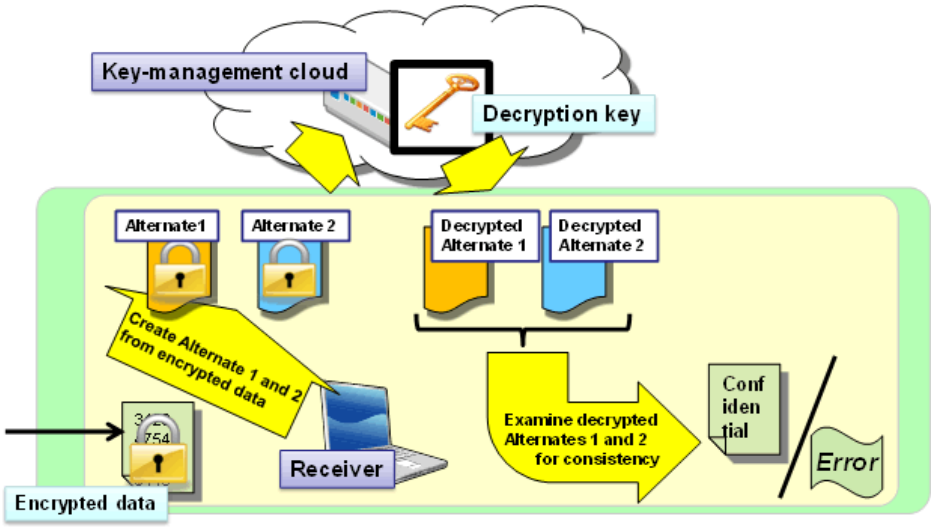

Figure 3: Self-correction technique developed by NTT Laboratories

3. Future developments

NTT plans to improve its prototype system for the cloud cryptographic scheme and continue its research on making this technology practical enough for business use by mass users. Specifically, NTT researchers will investigate ways of ensuring safety in the actual use of this cloud cryptographic scheme from both system design and operation viewpoints while also studying the social role of this technology. This research is planned to achieve a practical, commercial system within two to three years.

Inquiries:

NTT Information Sharing Laboratory Group
PR Section, Planning Department
E-mail: islg-koho@lab.ntt.co.jp

Information is current as of the date of issue of the individual press release.
Please be advised that information may be outdated after that point.

NTT Press Releases Index

NTT Press Releases

Latest Press Releases

Back Number

Japanese is here

Search Among NTT Press Releases

January 1997 - November 2021

Search

▲ Page Top

▸Recent updates ▸Site Map ▸Copyright ▸Privacy Policy ▸Contact