December 12, 2019

National Institute of Information and Communications Technology
Kochi Health Science Center
Kochi University of Technology
ZenmuTech, Inc
Shibaura Institute of Technology
SBS Information Systems Co., Ltd
SKY Perfect JSAT Corporation
NEC Corporation
ISARA Corporation
Technische Universität Darmstadt

Press Release

Demonstration of Secure Data Backup of Medical Records Using Secret Sharing on Secure Communications Network

- Prompt restoration of medical records via a satellite link for disaster medical support -

[Highlights]

- Secure data backup of medical records based on secret sharing
- Restoration of medical records via a satellite link within 9 sec after searching a patient ID
- Cross reference of medical records between different organizations using standardized data format

The National Institute of Information and Communications Technology (NICT, President: Hideyuki Tokuda, Ph.D.), Kochi Health Science Center (KHSC, Director: Yasuhiro Shimada) and collaborating teams have developed a secure data backup system in an 800 km network connecting the data servers in Kochi, Osaka, Nagoya, Otemachi and Koganei, Japan, using secret sharing*1 and secure communications technologies*2, and demonstrated distributed storage of medical records and prompt restoration of important items, such as prescription records and allergy information, via a satellite link within a time as short as 9 sec.

This technology would be useful for medical support in disaster situations as well as sharing and cross referencing medical records between various hospitals in ordinary situations.

The results will be presented in the session of quantum communication on December 16 in the EU-USA-Japan International Symposium on Quantum Technology 2019 held in Kyoto, Japan.

[Background]

In the Great East Japan Earthquake in 2011, many medical institutions were destroyed and data servers storing medical records were washed away by tsunami waters. It was then recognized that medical records should be backed up in remote places safely for such contingencies. In the case of emergency care after a disaster, medical examinations and treatment should be given to many people in a short time. During these times, there is a need to promptly restore a minimum of necessary items to profile a patient, such as prescription records and allergy information.

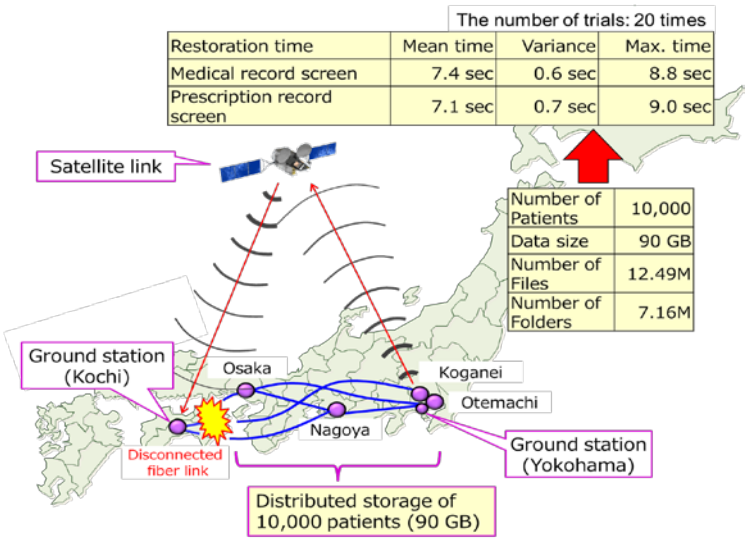

Figure 1: Network configuration of H-LINCOS and experimental results

Medical records are highly confidential personal information. Therefore, the backup of medical records should be protected by appropriate security techniques. Furthermore, if the backup conforms to a common standardized data format, they can be shared and cross referenced by many medical institutions to prevent duplicated examination and excessive medication as well as to develop new medical technologies.

So far, no techniques have been available which satisfy all these requirements at once.

[Achievements]

We combined secret sharing and secure communications technologies to realize a secure data backup system and demonstrated distributed storage of medical records and prompt restoration of important items, such as prescription records and allergy information, via a satellite link. This system is referred to as the Healthcare Long-term INtegrity and Confidentiality protection System (H-LINCOS).

This H-LINCOS has been implemented in an 800 km network connecting the data servers in KHSC, and the access points of a high-speed R&D network testbed called JGN operated by NICT, which are located in Osaka, Nagoya, Otemachi, and Koganei (see Figure 1. An enlarged version is also shown in the end of appendix.). To realize highly secure access control to the H-LINCOS, authentication functions are also implemented, using next generation technologies of quantum-safe public-key cryptography, which is expected to be secure even against quantum computer attacks.

In this experiment, sample data of medical records of 10,000 patients were provided by KHSC, whose total data size was 90 GB, converted into the standardized data format for medical information exchange (SS-MIX)*[3], and stored in a distributed manner in the H-LINCOS. In the demonstration of data recovery, we assumed that the Kochi area was damaged by a disaster, and terrestrial communication links to the Kochi area were disconnected. Under this scenario, a satellite link provided by SKY Perfect JSAT was introduced to the H-LINCOS connecting the ground stations in Yokohama and KHSC. Upon a query for a patient data item from a terminal device in KHSC, the original data was first restored in the Koganei data server by combining data pieces from two data servers in Osaka, Nagoya or Otemachi. The restored data was then sent to the Yokohama ground station, relayed to the KHSC ground station via the satellite link, and finally delivered to the terminal device in KHSC.

We could successfully restore important items, such as prescription records and allergy information, and display them on a screen within a time as short as 9 sec after the query. An allowable time to wait for information acquisition in emergency medicine is typically 15 sec. Our result satisfied this criterion. Our technology enables prompt delivery of medical information in disaster situations. It also provides a means to share and cross reference medical records between various hospitals in ordinary situations.

[Future Prospects]

We will further improve the performance and the reliability of the H-LINCOS. In particular, we will analyze communication latencies and H-LINCOS congestion when the stored data size and the number of connected terminal devices to access increase. We will also investigate efficient healthcare support in disaster situations by jointly operating the H-LINCOS and the Disaster/Digital information system for Health and well-being (D24H)*[4].

Publication of our results

Our results will be presented in the session of quantum communication on December 16 in the EU-USA-Japan International Symposium on Quantum Technology 2019 held in Kyoto.

Title: Quantum enhanced communication and cryptography
Speaker: Masahide Sasaki (NICT)
URL: https://www.jst.go.jp/kisoken/crest/isqt2019/index.html

Roles and tasks of our team members

- NICT: Grand design and implementation of H-LINCOS, conducting the experiment and managing the project
- Kochi Health Science Center: Derivation of requirements for H-LINCOS and providing sample data of medical records
- Kochi University of Technology: Derivation of requirements for H-LINCOS and design of secret sharing scheme
- ZenmuTech: Development of fast secret sharing driver software
- Shibaura Institute of Technology: Optimization of H-LINCOS for disaster medical support via D24H
- SBS Information Systems Co., Ltd: Development of medical record viewer
- SKY Perfect JSAT Corporation: Providing a satellite link
- NEC Corporation: Implementation of secure communication channels between the KHSC and Koganei access points
- ISARA Corporation: Development of quantum-safe public-key infrastructure for healthcare
- Technische Universität Darmstadt: Development of long-term secure integrity protection scheme

Glossary

***1 secret sharing**

Technique to create new multiple (say n) data (shares), each of which is of no use on its own, from an original data, and store the shares in different storage servers (shareholders) in a distributed manner. In a (k, n)-threshold scheme, the original data is restored by collecting at least k ($\leq n$) of shares. With shares of k-1 or less, the original data can never be reconstructed, even with unlimited computing power. Provided that the number of corrupted shareholders is less than k, and shares are exchanged through private channels, the (k, n)-threshold scheme ensures information theoretic confidentiality of storage. Even if shares up to n- k are lost, the original data can be reconstructed by using the k remaining shares, which provides availability of data.

***2 secure communication technology**

Technique to protect the confidentiality of transmitted data by using appropriate cryptographic methods. Symmetric key ciphers are commonly used at present. This scheme is, however, threatened by advances of computing technology. Recently quantum cryptography has become available, which can remain secure even against any computing technologies, ensuring information theoretical security.

***3 SS-MIX：Standardized Structured Medical Information eXchange**

Standardized data storage structure for exchanging medical information between medical institutions specified by the program called Standardized Structured Medical Information eXchange (SS-MIX) by Japan's the Ministry of Health, Labor and Welfare. The SS-MIX data format is based on hierarchical folder structure based on patient ID.

***4 disaster/Digital information system for Health and well-being (D24H)**

A system to provide necessary information for decision making on disaster healthcare support by gathering, integrating, and analyzing various information from the Shared Information Platform for Disaster Management (SIP4D) system managed by Ministries and individual systems operated by rescue teams and medical support teams.

Acknowledgements

A part of this work was performed by the Council for Science, Technology and Innovation (CSTI), the Cross-ministerial Strategic Innovation Promotion Program (SIP), the "Photonics and Quantum Technology for Society 5.0" (Funding agency: QST) and "Enhancement of National Resilience against Natural Disasters" (Funding agency: NIED).

Appendix

1. Technical details on H-LINCOS

In H-LINCOS, medical record data is backed up using secret sharing as depicted in Figure 2. First, medical record data is converted to SS-MIX data. Next, the original SS-MIX data is converted into multiple data called shares, each of which is of no use on its own. Finally, the shares are distributed to remote data servers via secure communication channels and stored in those data servers.

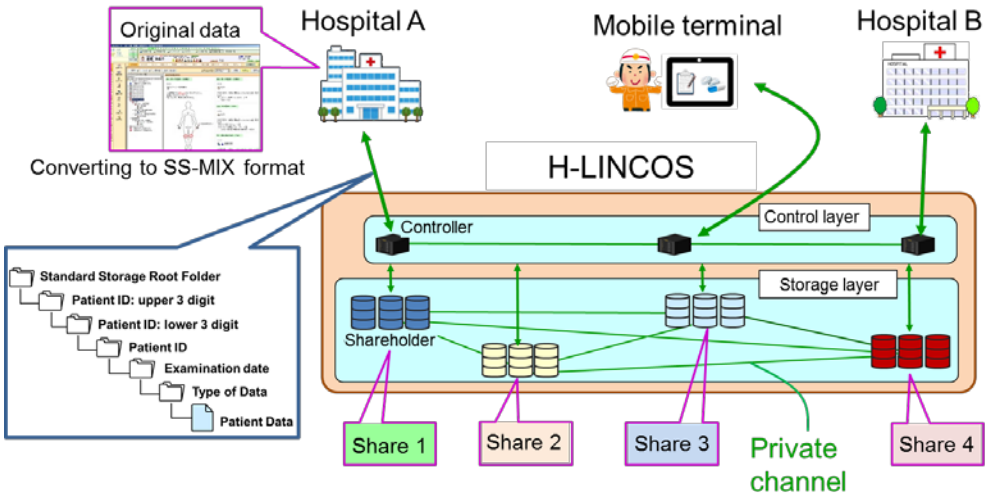

Figure 2: Conceptual structure of H-LINCOS

With this method, even if some servers have crashed or are lost, the original data can be restored from the remaining servers. On the other hand, the original data cannot be restored unless a certain number of distributed data are gathered. Therefore, the confidentiality of the data can be enhanced, enabling ***secure backup***. In addition, by conforming to SS-MIX, it is possible to ***cross-reference medical record data***. Moreover, we developed data access technology for high-speed search, a so-called fast secret sharing driver, and realized ***rapid restoration of important data items of medical records required in disaster situations***.

In our implementation, the SS-MIX data provided by KHSC was first transmitted over an 800 km secure channel to the Koganei access point on JGN. It was then converted to shares. They were then distributed to data servers in the Osaka, Nagoya, and Otemachi access points via secure communication channels, and stored there.

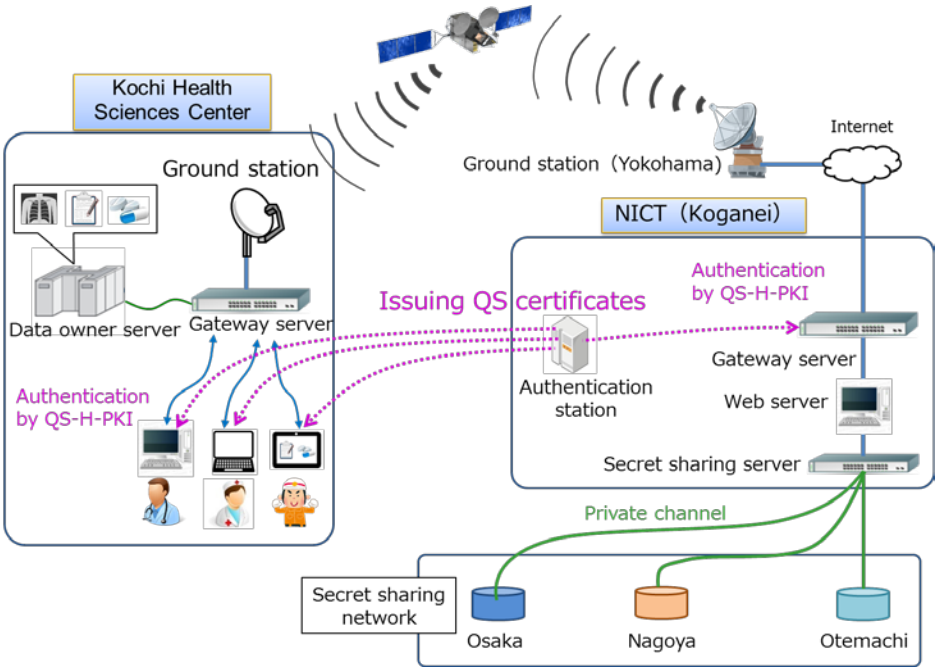

Figure 3: Configuration of access control scheme based on quantum-safe PKI

The secret communication channel consists of a symmetric key cipher seeded with a pre-shared physical random number pair. Its security is "quantum-computer resistance", which is difficult to decrypt even with quantum computers. In the KHSC and Koganei access points, NEC's symmetric key cipher system was installed, which enables high-speed encryption at the data link layer. In addition, in the 100 km area of Tokyo, including Otemachi and Koganei, a quantum key distribution network was used to realize secure communication, which allows secret sharing with "information theoretical security" that cannot be decrypted by any computer.

Access control for the H-LINCOS is executed by using highly secure user authentication and access right management based on national qualifications for healthcare workers. More precisely, the access control scheme is designed by following the Healthcare Public Key Infrastructure (H-PKI) recommended by the Ministry of Health, Labor and Welfare. Furthermore, a next generation scheme of PKI based on quantum-safe public-key cryptography is newly introduced to increase the security to a level of quantum-computer resistance, making it difficult to decipher even with a quantum computer. This so-called quantum-safe H-PKI (QS-H-PKI) is depicted in Figure 3.

As quantum-safe public-key cryptography, we selected seven schemes that are expected to be promising in the standardization process currently underway by the National Institute of Standards and Technology (NIST). Specifically, combining two hash-based schemes for issuing root certificates, two schemes (lattice-based and isogeny-based) for key exchange, and three schemes (two lattice-based and one multivariate-based) for digital signature, a total of 12 types of cryptographic tool sets (so-called cipher suites) were prepared. These were implemented in compliance with the Internet standard Transport Layer Security (TLS). It was confirmed that all cipher suites operate normally with a processing time of about 100 to 250 ms. Although this processing speed is about 10 times that of the existing TLS, it is sufficiently practical for our purpose. In our SS-MIX data restoration experiment using a satellite link, the fastest cipher suite was adopted for access control.

In restoring SS-MIX data assuming a disaster situation, two data servers in Osaka, Nagoya, or Otemachi, were selected, and data items such as prescription records and allergy information were restored in the Koganei server. The data was then sent to the SKY Perfect JSAT ground station in Yokohama via a secret communication channel on the Internet, transmitted to the KHSC ground station via the satellite link, and finally restored in the medical viewer terminal in KHSC.

2. Experimental results

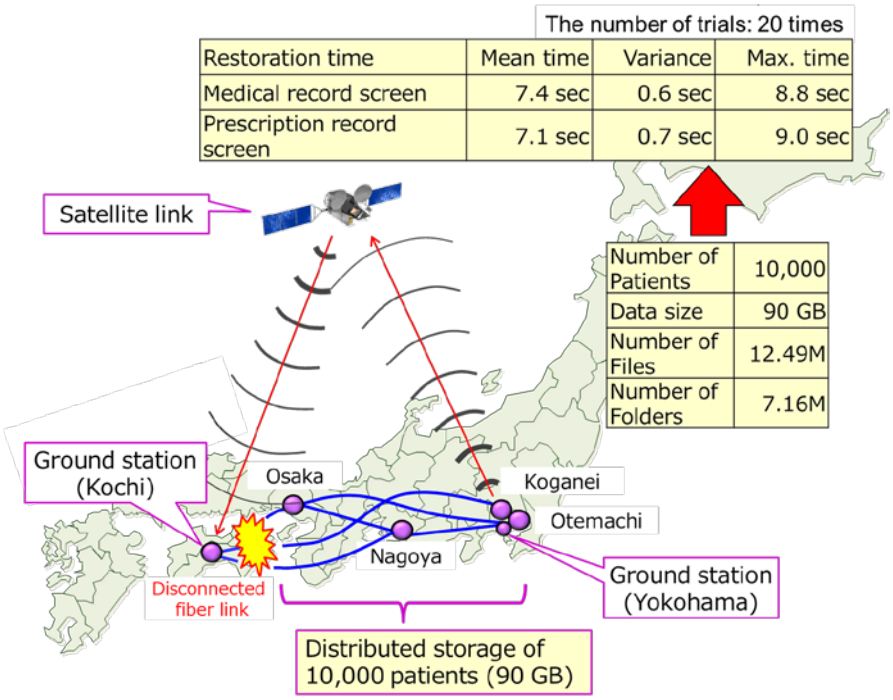

Figure 1: Network configuration of H-LINCOS and experimental results. (An enlarged version)

Conducting 20 restoration campaigns, we confirmed that the average time from entering the patient ID to displaying the medical record viewer screen was 7.4 seconds, the maximum was 8.8 seconds, and the time from clicking the prescription record selection button to displaying the contents was 7.1 seconds on average, and the maximum was 9.0 seconds (see Figure 1).