PHYS ORG

Inter-cloud data security technology developed by Fujitsu

October 19 2010

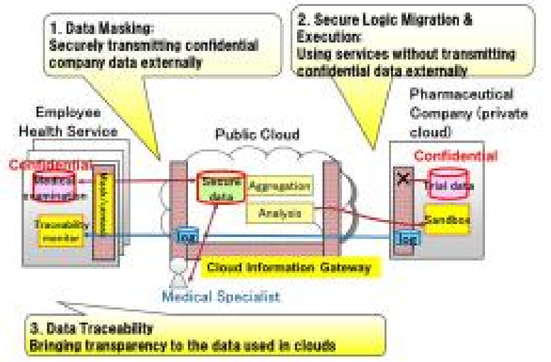
1. Data Masking:
Securely transmitting confidential company data externally
2. Secure Logic Migration & Execution:
Using services without transmitting confidential data externally
Employee Health Service
Confidential
Traceability monitor
Public Cloud
Secure data
Aggregation
Analysis
log
Cloud Information Gateway
Medical Specialist
Pharmaceutical Company (private cloud)
Confidential
Trial data
Sandbox
log
3. Data Traceability
Bringing transparency to the data used in clouds

Figure 1: Usage Scenario for Newly Developed Data Gateway

Fujitsu Laboratories Limited today announced the development of security technology that enables confidential data to be safely shared among different computing clouds.

With the advent of cloud computing, the boundary separating internal and external data has become increasingly blurred due to the utilization of external services. As a result, existing methods of preventing data leakage, such as only using a gateway to block the outflow of confidential data, have become insufficient, and there is increased demand for new security technology to allow the safe use of confidential data even in the cloud.

Fujitsu has developed new cloud information gateway technology that masks confidential information contained within data before it is processed in the cloud and that transfers applications from the cloud to inside the company for internal processing, thereby making it possible to utilize cloud services without transmitting actual data. This technology enables users to safely utilize confidential data in the cloud, encouraging new uses of cloud computing, such as cross-industry collaborations and specialized uses in specific industries.

Details of this technology will be presented at *Computer Security Symposium* 2010 (CSS2010), to be held starting October 19 in Okayama Prefecture, Japan.

With the rapid adoption of cloud computing-based services, an increasing number of users are expected to employ clouds to safely utilize confidential data as part of cross-industry collaborations. Currently, users have to choose between the confidentiality offered by private networks and the convenience offered by the cloud, but increasingly they will have to entrust clouds with confidential data.

Until now, Fujitsu Laboratories has developed technology to prevent the unwanted disclosure of various data, including preventing leaks from paper-based materials and data stored in USB memory devices. In anticipation of the age of cloud computing, however, new technology to prevent information leaks is becoming necessary.

Existing techniques for preventing information leaks include encryption and the blocking of the outflow of confidential data before it reaches a company's external boundary. In the age of cloud computing, however, the boundary separating internal and external data has become increasingly blurred due to the utilization of external services. As a result, services cannot be employed if a user simply blocks or encrypts classified data. Furthermore, such methods would make it impossible for multiple companies to securely use each other's data in the cloud.

In order to address the aforementioned challenges, Fujitsu Laboratories developed new cloud information gateway technology that can flexibly control data, including data content, transmitted from the inside of a company to a cloud and between multiple clouds. In addition to the option of blocking confidential data, the data gateway also includes the following three features.

1. Data Masking Technology

Using masking technology, when data passes through the information gateway, confidential parts of the data can be deleted or changed before the data are transmitted to an external cloud. For example, the technology can be used to temporarily conceal personal information inside of a medical examination record with pseudonyms before sending it to an external industry-wide cloud for examination by a medical specialist. When the results from the examination have been received, the data can once again be restored to their original form.

In addition, with confidential numerical chart data, such as a breakdown by region of patients suffering from a certain disease, special operations can be performed on the data to mask the original figures before sending the data to the cloud, making it possible for multiple data sets to be aggregated without any modifications (patent pending). Each user can obtain access to different levels of detail for the tallied results using decryption keys that grant different levels of access (prefecture level, city level, town level, etc.). Processing is possible without needing to store actual data or keys in the cloud, and, in addition, the data can be accessed by users on multiple levels based on a single data set, making database management easy.

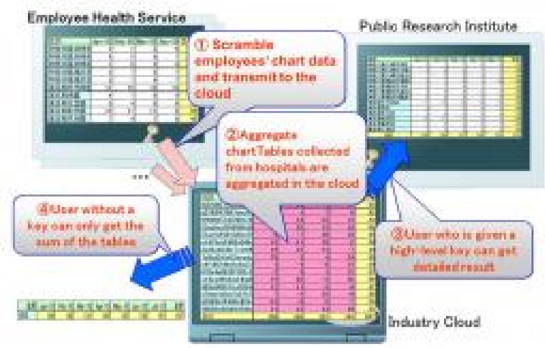
Employee Health Service
① Scramble employees' chart data and transmit to the cloud
Public Research Institute
②Aggregate chartTables collected from hospitals are aggregated in the cloud
④User without a key can only get the sum of the tables
③User who is given a high-level key can get detailed result
Industry Cloud

Figure 2: Example of Masked Aggregation of Statistical Chart Data

2. Secure Logic Migration and Execution Technology

For confidential data that cannot be released outside of the company, even formed by concealing certain aspects of the data, by simply defining the security level of data, the information gateway can transfer the cloud-based application to the in-house sandbox for execution. The sandbox will block access to data or networks that lack pre-authorized access, so even applications transferred from the cloud can be safely executed. Moreover, because the execution status of applications is recorded, application providers are able to confirm if there is any inappropriate use of the data.

3. Data Traceability Technology

The information gateway tracks all information flowing into and out of the cloud, so these flows and their content can be checked. Data traceability technology uses the logs obtained on data traffic as well as the characteristics of the related text to make visible the data used in the cloud. For example, in a joint development project, one can check how textual data collected in the cloud have been used, including whether portions have been copied, thereby enabling any inappropriate usage to be identified.

With the newly developed cloud gateway, confidential data can be securely handled in the cloud without users or application developers having to take special precautions to guard data confidentiality. Depending on the circumstances, data can either be masked or the cloud-based processing application will be executed in-house, and therefore confidential data are not physically transferred to the cloud. Because the information gateway limits data flowing into or out of the cloud, movements of data in the cloud traffic flows can be made visible, and it is possible to block the transfer or copying of data to unintended destinations. These functions will be essential for cases in which private data are being handled in the cloud or for collaborations in which multiple organizations are developing new products.

This technology will now undergo verification in environments where multiple clouds are working in collaboration, with commercialization targeted for 2012.

Provided by Fujitsu

Citation: Inter-cloud data security technology developed by Fujitsu (2010, October 19) retrieved 25 April 2024 from https://phys.org/news/2010-10-inter-cloud-technology-fujitsu.html