World's first encryption technology able to match multi-source data encrypted with different keys

February 16 2016

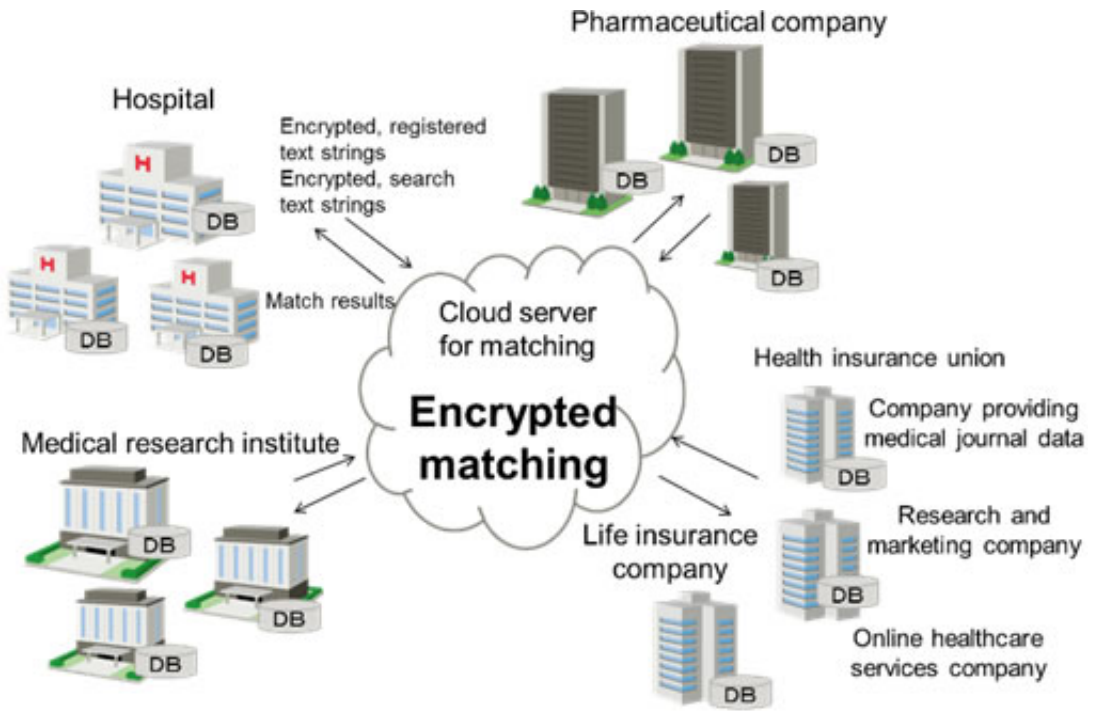

Figure 1. Data linkages in the medical and pharmaceutical fields

Fujitsu Laboratories today announced development of the world's first encryption technology that can match IDs or attribute values in information sources, such as classified or private data from multiple organizations, that are encrypted with different keys, without decrypting the information. With previous encryption technologies that could search

and compute data while still encrypted, encryption and decryption of search results used the same key, creating issues when used among organizations.

Now, Fujitsu Laboratories have developed an encryption technology that can match the data of various organizations that was encrypted with different keys, and can determine the results of this matching for a specified group of organizations. Data cannot be decrypted with the key used for matching, so sensitive information from multiple organizations can be matched in a cloud environment while preserving confidentiality, such as in linking examination information and diagnosis records among multiple hospitals, for example. This technology will be exhibited at Fujitsu North America Technology Forum 2016 (NATF 2016), which will be held in Santa Clara, California, on Tuesday, February 16th.

Development Background

As the use of the cloud and big data analysis has progressed, there has been an increasing demand for the shared use of personal data and confidential information among multiple organizations. For example, in the healthcare field, there is a movement underway to use clinical, health, and genome information, among others, and tie it into the clinical studies or the drug-discovery business among multiple research organizations (Figure 1). From the perspective of preserving privacy, however, there is also a need to limit the use of shared data in the cloud, and to maintain the secrecy of the data being searched when linking sensitive data.

Issues

Several methods exist for matching IDs and attributes while maintaining confidentiality. One is the hash function, which is a data transformation

method widely used for checking whether passwords match, and another is homomorphic encryption, which enables addition, multiplication, and searching of data while it is still encrypted. With hash functions, it is difficult to restore original data, but the same data is always transformed into the same value, so, when dealing with only a few data types, there is a possibility that the original data can be analogically inferred. With homomorphic encryption, it is necessary for all organizations to use the same encryption key. While search results are encrypted, the key necessary to decrypt the search results can also decrypt all of the data, so it is necessary to strictly manage the key. Therefore, there has been a need for safer encryption technology for matching data shared among multiple organizations.

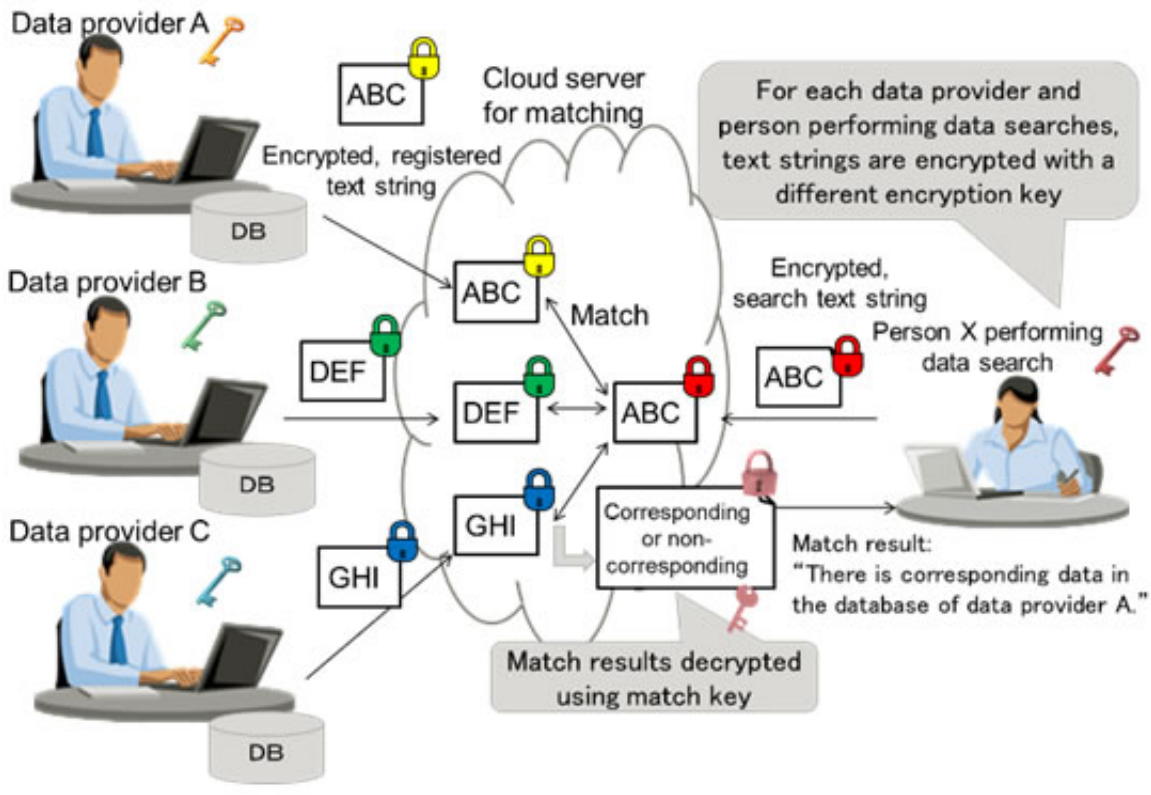

Figure 2. Anonymized searches in the cloud using different encryption keys

Newly Developed Technology

Fujitsu Laboratories and Fujitsu Laboratories of America have now developed the world's first encryption technology that enables the matching of data from different organizations while still encrypted. The newly developed technologies are as follows:

1. Technology that matches text strings encrypted with different keys through the cloud

Based on the theory of relational cryptography, a concept devised by Fujitsu Laboratories of America that calculates the degree to which encrypted information matches, Fujitsu Laboratories and Fujitsu Laboratories of America developed technology that can determine a match between text strings encrypted with different encryption keys (figure 2). With this technology, registered strings and search strings are encrypted with the encryption key of each organization. A registered string can be compared with the search string to see if they correspond while still encrypted, on a cloud server used for matching. The strings are encrypted with a one-way function which has similar effects to a hash function, so they cannot be decrypted even with the keys used to encrypt them. The matching results are also encrypted, and can only be seen by a person holding a dedicated match key.

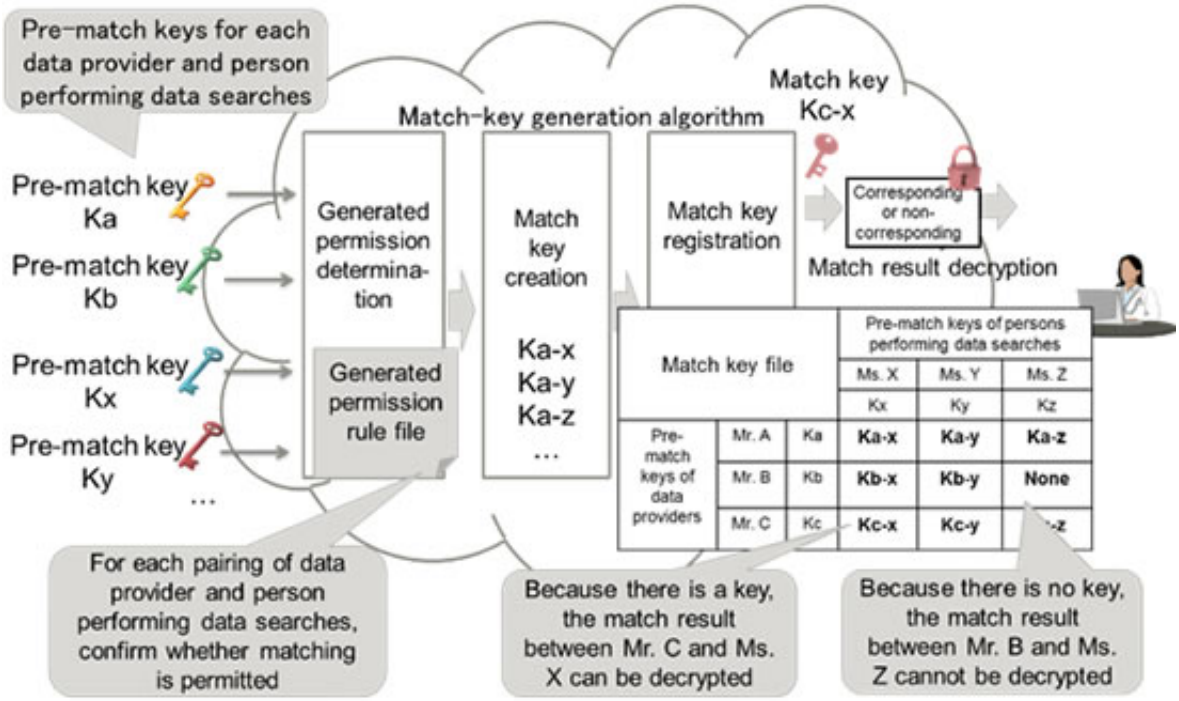

Figure 3. Match key scheme

2. Access control technology enables users to choose who is allowed to run matches

Fujitsu Laboratories and Fujitsu Laboratories of America have developed a technology that can flexibly control match permissions in the cloud, with which the match key for confirming match results is created from specific keys (pre-match keys) transmitted to the cloud for both data providers and the person performing the search (figure 3). The data provider creates rules governing which people can conduct matching, and can create and manage match keys for pairings of providers and searchers in the cloud on the basis of these rules.

Effects

In internal tests conducted by Fujitsu Laboratories, it was confirmed that one pair of text strings could be matched in 0.02 of a second using a typical PC. By applying this technology to genetic data or other medical data, for example, medical research institutes or pharmaceutical companies could see whether the information they need is included in a registered database while keeping patient data anonymized. Such applications are expected to support the diagnosis of rare diseases and create efficiencies in new drug discoveries. This technology also enables near matches, which allow for a difference of a few bits in the text strings. It can also be applied beyond the medical field, to a variety of search scenarios involving data that previously was the subject of concerns about leaks, such as personal data or company secrets, in such fields as finance, education, public administration, marketing, and patent investigations. The technology enables secure data links that transcend organizational boundaries.

Fujitsu Laboratories will work on compressing the data size and accelerating the speed of this technology, with the aim of bringing it into practical implementation in fiscal 2016.

Provided by Fujitsu

Citation: World's first encryption technology able to match multi-source data encrypted with different keys (2016, February 16) retrieved 10 April 2024 from https://phys.org/news/2016-02-world-encryption-technology-multi-source-encrypted.html