NRI

Iakyara vol.348

Secure computation is a boon for data-driven businesses

Yasunori Hokazono

10.Nov.2021

Nomura Research Institute, Ltd.

Yasunori Hokazono
Senior Researcher
Digital Wholesale Finance Platform Department

Executive Summary

Encryption technologies that allow computations to be performed on encrypted data without decryption have enabled new services that were previously not possible, including needs matching and outsourced computation that maintain data confidentiality. These secure computation technologies should help financial institutions utilize their vast data troves, including personal information.

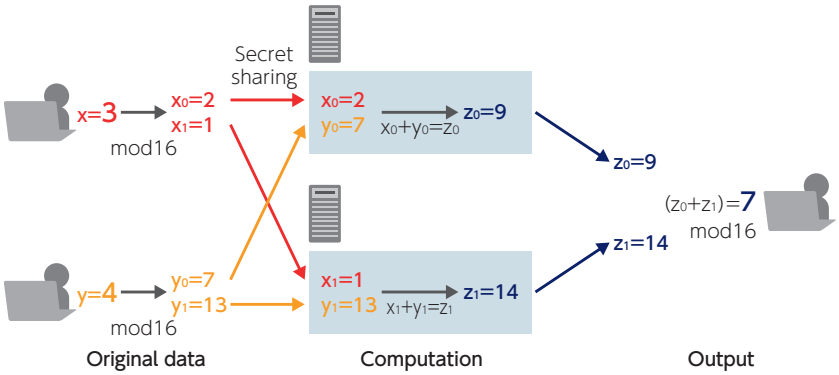
Secure computation is a technology that enables computations to be performed on encrypted data without first decrypting the data. Encryption technologies were originally developed out of a need to protect data while in transit. Secure computation goes a step farther by allowing data owners to keep their data confidential from contractors to which they outsource data for analysis/computation. With secure computation, the data owner provides data to the contractor in encrypted form. The contractor performs the requested computations without decrypting the data and delivers only the computational output to the data owner. This approach affords more privacy to both the data owner and contractor.

Secure computation is already being used for a number of use cases, including commodity auctions, analysis of individuals' income and educational backgrounds and management of cryptographic keys. Following is a brief introduction to how secure computation works.

Implementation of secure computation

The most common implementation of secure computation is based on homomorphic encryption and multi-party computation (MPC). Fully homomorphic encryption (FHE) supports both addition and multiplication operations, whereas partially homomorphic encryption supports only one or the other. FHE's ability to simultaneously support both addition and multiplication means that secure computation can perform all arithmetic operations that a computer can. One drawback of FHE, however, is that it is computationally expensive when complex computation is involved.

Example of computation of 3 + 4 = 7 using secret sharing



MPC is a cryptographic technology that uses secret-sharing to increase security by fragmenting data into the hands of multiple parties in different locations. Because the data fragments are meaningless individually, the original data would not be compromised even if one of the fragments were stolen. To be decrypted, the distributed data fragments must be gathered in one location. When computations are performed on data fragments stored across multiple servers through secret sharing, the servers communicate with each other. The intended computational output can be decrypted by aggregating all of the servers' respective outputs. While the need for a set of networked servers poses a challenge, MPC-based secure computation is computationally fast.

Utilization of personal information in companies' possession

Secure computation is applicable to financial institutions and nonfinancial companies' use of the data in their possession. In Japan, a major transportation carrier is utilizing secure computation on its data, including passenger travel and purchase records, to upgrade its passenger flow analysis and marketing.

Financial institutions are expected to likewise utilize personal information, including customers' deposit and securities account balances, for marketing and advertising purposes in pursuit of business opportunities. If so, they will likely use secure computation when analyzing or utilizing personal information for any purpose not originally intended. However, Japanese financial institutions will have to wait for more clarity from the Personal Information Protection Commission, which is discussing issues around handling of encrypted personal information, including whether encryption impersonalizes personal information.

One way to bypass restrictions on use of personal information for purposes not originally intended is data anonymization. Data are anonymized through such means as deletion of personal identifiers like names and ID numbers and generalization of demographic attributes into ranges or groups. Anonymization renders data subjects unidentifiable. Additionally, anonymized data cannot be restored to the original personal information. Anonymization thus lowers the bar to sharing data with third parties and using data for purposes not originally intended while also enabling statistical and trend analysis.

Secure computation's use cases include not only solo use by single companies but also joint use by multiple companies within the same industry. In the latter case, what is shared among the companies is not the companies' data but statistical information or an AI model. As an example, financial institutions are jointly building an AI model to detect fraud and other illegalities in withdrawals, remittances and other transactions as a social experiment. While no single financial institution has much fraudulent/illegal transaction data, the participating financial institutions have expanded their AI training dataset and, in turn, improved AI accuracy by teaming up with each other. Because they are not sharing data with each other, data security is high.

Use in bilateral trading markets

Another use case for secure computation is in bilateral trading markets like real estate. In the real estate market, there is strong demand for brokers who seek out counterparties (buyers or sellers) for their clients without divulging certain information such as their client's identity, property details and/or the price their client is willing to pay or accept. If a secure computation platform were available in the real estate market, sellers would share encrypted property information with the platform while buyers would encrypt information on their preferred deal parameters (e.g., price, location). The platform would then perform secure computation to match sellers and buyers. If the platform were set up like this, not even the administrator or platform operator would be able to access the property information or deal-parameter preferences. Certain real estate brokerages are working on implementing such a platform. Though many challenges remain to be addressed, real estate broking is a promising use case.

Other use cases with potentially even more promise include digital assets, business succession, M&A and auctions. Combining secure computation with

blockchain technology in particular would prevent fraud, forgery and other illegalities more effectively and increase the platform's value as a trading venue.

Protecting privacy with secure computation

With data proliferating throughout society and data distribution costs decreasing, data sharing and utilization offer many benefits to society, as clearly evidenced by the large profits that online platforms and portal sites are reaping from their advertising businesses by analyzing cookie data and site traffic.

Users, however, have little if any control over their own data and no assurance that their privacy is fully protected within such online cloud services. Secure computation is expected to rectify such shortcomings and privacy concerns as social infrastructure for data sharing/utilization.

It is imperative for financial institutions and other companies that possess a lot of personal information to analyze and utilize that information and share it across industry boundaries. In doing so, they need to take full advantage of encryption technologies to protect privacy while building data-driven businesses.

about NRI

Founded in 1965, Nomura Research Institute (NRI) is a leading global provider of system solutions and consulting services with annual sales above $4.9 billion. NRI offers clients holistic support of all aspects of operations from back- to front-office, with NRI's research expertise and innovative solutions as well as understanding of operational challenges faced by financial services firms. The clients include broker-dealers, asset managers, banks and insurance providers. NRI has its offices globally including New York, London, Tokyo, Hong Kong and Singapore, and over 13,000 employees.

For more information, visit https://www.nri.com/en

Inquiries to : Financial Market & Digital Business Research Department
Nomura Research Institute, Ltd.
Otemachi Financial City Grand Cube,
1-9-2 Otemachi, Chiyoda-ku, Tokyo 100-0004, Japan
E-mail : kyara@nri.co.jp

https://www.nri.com/en/knowledge/publication/fis/lakyara/