END-TO-END PROTECTION FOR SENSITIVE DATA

CUTTING-EDGE CRYPTOGRAPHIC TECHNIQUES being developed in Japan promise a world where personal and sensitive information remains secure throughout its lifecycle.

In an interconnected world where data breaches and privacy concerns have become all too common, a prominent research entity in Japan is spearheading a transformation of the data security landscape.

NTT Social Informatics Laboratories, part of the central research and development arm of the country's largest telecommunications company, NTT, is conducting pioneering cryptography research aimed at ensuring a high level of security for personal and sensitive information throughout collection, transmission, storage and computation.

"Our objective is to establish a world without plain text, where cryptography is applied end-to-end, ensuring that personal information is never decrypted from its inception to its disappearance," says Daigoro Yokozeki, project manager for Privacy Enhancing Computing and Data Sharing, at NTT, based in Tokyo.

EHHANCED PRIVACY

Yokozeki and his team are actively working on privacy-enhancing computation (PEC) techniques that allow secure, encrypted data to be processed and analysed without decrypting it back to plain text. This approach protects the data from exposure during computation, as well as transmission and storage, enabling the secure interconnection of data centres across different locations and facilitating real-time data processing.

One potential application of PEC techniques lies in the analysis of healthcare data, particularly in the context of large-scale data collection and analysis by medical institutions.

In this scenario, personal healthcare information is encrypted on the collection device — such as a smartphone — and securely transmitted to an online data store in the cloud. PEC allows computations to be performed on the encrypted data in secure and encrypted environment, ensuring there is no risk that the security of the data could be compromised.

"In conventional computation, once digital data is captured, there is no guarantee of how it will be utilized," explains Yokozeki. "With PEC, neither the cloud administrator nor the medical institution itself can access the raw unencrypted data. The medical institution can only access pre-approved statistical or analytical results agreed on in advance with the individual who provided the data, which serves as an enhanced form of data governance."

This innovative approach enables users to have confidence that their personal health information can be shared securely with healthcare professionals, empowering providers to deliver personalized and effective treatments, while maintaining the privacy and confidentiality of their personal medical history.

Andrew Brookes/Image Source/Getty

ADVERTISEMENT FEATURE

SECURE COMPUTATION

Building on its more than 40 years of research and development on state-of-the-art cryptography, NTT has now developed a secure computation platform that allows computation using encrypted data without the need for decryption.

"Compared to conventional computation directly on plain text, computation on encrypted data is usually much slower due to computational overhead," says Ryo Kikuchi, a research engineer in secure computation technology at NTT.

This computational overhead is one of the major challenges associated with developing algorithms capable of efficiently performing computations on encrypted data. Kikuchi and his team, however, have developed some of the fastest known methods for carrying out statistical analysis, joining relational databases, machine learning and artificial intelligence modelling directly on encrypted information. The result is a reduction in computational overhead to that comparable for raw data such as plain text.

"Our focus is on custom-designing algorithms for our cryptography to efficiently evaluate more advanced analytics that may be required for real-world use cases," Kikuchi says.

The team is continuing to work on optimizing complex functions for use on ever-larger datasets, as well as progressing standardization, which will become important to promote the widespread adoption of PEC.

SECURE DATA SHARING

As we increasingly rely on smart devices, the 'Internet of Things' and artificial intelligence, the need for robust data protection becomes ever more critical. Researchers and organizations are continually seeking innovative solutions to protect sensitive information while enabling secure data sharing. One such technological advancement that has gained significant attention is the Trusted Execution Environment (TEE).

"TEE utilizes the hardware features of the CPU to prevent platform operators or host operating system owners from accessing raw data held in computational memory," says Tomohiro Inoue, who leads the development of NTT's PEC platform using TEE technology, working alongside Yokozeki. "Our approach is unique in that it can also accommodate more than three parties, such as the data owner, those who process the data and those who use the processed results."

This multi-party cryptographic environment makes it possible to share and process data under full encryption while enabling collaboration — something that has been very difficult to achieve practically.

Inoue's team at NTT is developing this feature as an extension of the Innovative Optical and Wireless Network (IOWN) — a global next-generation network and computing infrastructure aimed at addressing the challenges posed by the rapidly increasing volume of data that needs to be stored, shared and secured.

"We are developing this feature to meet the requirements of data usage control proposed by the International Data Spaces Association, which is dedicated to secure data distribution protocols among data users in the European Community," adds Inoue. "Currently, we are engaged in discussions regarding the use of TEE to ensure compliance with data usage control requirements within their systems."

▲ **Data security researchers Ryo Kikuchi, Daigoro Yokozeki and Tomohiro Inoue (left to right) are leading NTT's development of an end-to-end data security ecosystem that keeps patient medical data encrypted for its entire lifecycle.**

The combination of IOWN with NTT's cryptographic technologies could enable high-volume encrypted data sharing between virtualized, distributed data centres.

FUNDAMENTAL CHANGE

Another major challenge being addressed by NTT Social Informatics Laboratories is guaranteeing proper use of the data. Through PEC incorporating TEE and secure computation technologies, it is possible to technologically guarantee that the data can only be used for the purpose permitted in advance by the data owner. Pilots of these cryptographic techniques are now underway in Japan for medical data sharing and genomic data analysis by universities using this permission framework.

Achieving true 'end-to-end' encryption, without the need for decryption at any point and with technologically guaranteed usage permissions, will fundamentally change how sensitive information is securely transmitted, stored, processed and analysed.

"The development of such ubiquitous PEC technologies will be truly significant," says Kikuchi.

He notes that while the concept of secure computation has been known for some time, its true potential and high-speed capabilities are only being realized now that previous limits on the computation power required for encryption have been overcome.

"Where encrypted computations were previously limited to simple addition and multiplication operations, our research enables us to handle complex operations, such as data integration and artificial intelligence applications," Kikuchi says. "This advanced capability will be crucial for analysing data across organizations. I believe we are at the forefront of real-world applications in this area." ■

NTT

www.rd.ntt/sil/project/iown-pec/

Advertiser retains sole responsibility for content