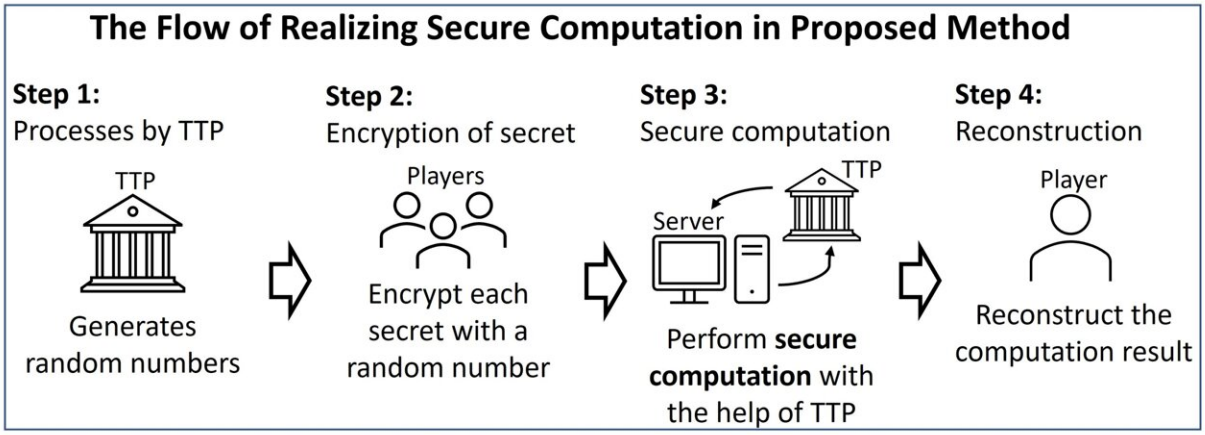
Improving data security for a hybrid society: Insights from new study

January 23 2023



Researchers at the Tokyo University of Science use a combination of TTP and various players to encrypt the data. However, all the computation is performed on a single server. Credit: Ahmad Akmal Aminuddin Mohd Kamal from Tokyo University of Science

Society 5.0 envisions a connected society driven by data shared between people and artificial intelligence devices connected via the Internet of Things (IoT). While this can be beneficial, it is also essential to protect the privacy of data for secure processing, transmission, and storage. Currently, homomorphic encryption and secret sharing are two methods used to compute sensitive data while preserving its privacy.

Homomorphic encryption involves performing computations on encrypted data on a single server. While being a straightforward method, it is computationally intensive. On the other hand, secret sharing is a fast and computationally efficient way to handle encrypted data. In this method, the encrypted data or secret input is divided and distributed among multiple servers, each of which performs a computation such as multiplication with its piece of data.

The results of these computations are then used to reconstruct the original data. In such a system, the secret can only be reconstructed if a certain number of pieces, known as the threshold, are available. Therefore, if the servers are managed by a single organization, there is a higher risk that the data could be compromised if the required number of pieces falls into the hands of an attacker.

To improve data security, it is ideal for multiple companies to manage computing servers in a decentralized manner such that each server is operated independently. This approach reduces the likelihood of an attacker gaining access to the threshold number of pieces required to reconstruct a secret. However, implementing this system can be challenging in practice due to the need for a fast communication network to allow geographically separated servers to communicate with each other.

This leads to an important question: is there a way to maintain data integrity without having to rely on independent servers, and without incurring a high computational cost?

In a study published on November 14, 2022, in Volume 10 of *IEEE Access*, Professor Keiichi Iwamura and Assistant Professor Ahmad A. Aminuddin of Tokyo University of Science, Japan, introduced a new secure computation method where all the computations are performed on a single server without a significant computational cost.

The system consists of a trusted third party (TTP), one computing server, four players who provide secret inputs to the server, and one player who restores the computation result. The TTP is a neutral organization that generates random numbers which are provided to the server (these are known as shares) and the players in certain combinations.

These random numbers are used to encrypt the data. Each player then performs a computation with the random numbers and generates secret inputs which are sent to a server. The server then uses the shares and secret inputs, along with new values computed by the TTP, to perform a series of computations, the results of which are sent to a final player who reconstructs the computation result. This method allows for the decentralized computation of encrypted data while still performing the computation on a single server.

"In our proposed method, we realize the advantage of homomorphic encryption without the significant computational cost incurred by homomorphic encryption, thereby devising a way to securely handle data," says Prof. Iwamura, who led the study and is the paper's first author.

Moreover, the method can also be modified such that the random numbers generated by the TTP can be stored securely by a Trusted Execution Environment (TEE), which is a secure area in a device's hardware (processor). As the TEE takes over the role of the TPP during the subsequent computational process, it reduces the communication time and improves the speed at which the encrypted data is handled.

As our society becomes more reliant on the internet, we are moving towards storing data on the cloud rather than locally. To securely manage the growing amount of data, it is important to have a reliable and efficient method of handling it. "We realize a method that addresses all

the drawbacks of the aforementioned methods, and it is possible to realize faster and more secure computations than conventional methods using secret sharing," says Assistant Prof. Aminuddin.

More information: Keiichi Iwamura et al, TTP-Aided Secure Computation Using (k, n) Threshold Secret Sharing With a Single Computing Server, *IEEE Access* (2022). DOI: 10.1109/ACCESS.2022.3222312

Provided by Tokyo University of Science