Client-Server Framework for Securely Outsourcing Computations

by Thijs Veugen (TNO)

In the current age of information, with growing internet connectivity, people are looking for service providers to store their data, and compute with it. On the other hand, sensitive personal data is easily misused for unintended purposes. Wouldn't it be great to have a scalable framework, where multiple users can upload personal data, which allows the servers to offer services on these data without ever revealing any data to the servers? TNO and CWI in the Netherlands have developed such a framework.

At first sight it might appear to be a magic trick, but with modern cryptographic tools it is actually possible to compute with data without ever learning the data itself. In a joint research effort [1], TNO and CWI have developed such a framework. Centrum Wiskunde & Informatica (CWI), with their state-of-the-art expertise on cryptography, fine-tuned existing techniques to the client-server setting. This enabled the Dutch organisation for applied scientific research (TNO) to implement and test such a framework for a particular application – in this case a recommendation system.

Secure computations. Source: Beeldbank TNO.

In recommendation systems, service providers can recommend products to their customers based on personal data from many users. To avoid leakage of these personal data, service providers use secret sharing. This enables them to compute the recommendation, while remaining oblivious to the contents. Only the user requesting the output will be able to combine all shares of the recommendation and learn the result.

Although similar secure recommendations systems have been developed before, they were either less secure, or less efficient. This framework is the first one that uses fast cryptographic techniques within a 'malicious security model'. By precomputing a lot of input independent data, the two servers were able to compute a recommendation within 0.34 seconds, using data from 10,000 users. The framework can be extended to an arbitrary number of servers, and as long as at least one behaves in an honest way, no data is leaked. Since secret sharing requires no additional cryptographic keys, the number of framework users is easily scaled up.

This secure client-server framework, which enables any kind of computation to be outsourced to the servers, is just one example of the applications of secure multi-party computation. In this field, many parties jointly compute a function on their private inputs without revealing the inputs to another party. Depending on which party is inputting data, which party receives the output, and which parties are doing the computations, many different applications are possible [2]. Some examples include: genomic research by biobanks, network anomaly detection by network administrators and financial reporting within a consortium.

TNO and CWI [L1, 2, 3] intend to extend the current work by exploiting techniques from the field of secure multi-party computation [3] within various application domains. This will open up unforeseen opportunities and collaboration models for organisations.

Links:

[L1] https://www.tno.nl/en/collaboration/expertise/early-research-programme/early-research-program-making-sense-of-big-data/
[L2] http://www.commit-nl.nl/projects/trusted-healthcare-services
[L3] http://projects.cwi.nl/crypto/

References:

[1] T. Veugen, R. de Haan, R. Cramer, F. Muller: "A Framework for Secure Computations With Two Non-Colluding Servers and Multiple Clients, Applied to Recommendations" IEEE TIFS, March 2015.
[2] P. Laud, L. Kamm: "Applications of Secure Multiparty Computation", CISS, 2015.
[3] R. Cramer, I.B. Damgård, J.B. Nielsen: "Secure Multiparty Computation and Secret Sharing", July 2015.

Please contact:

Thijs Veugen
TNO, The Netherlands
thijs.veugen@tno.nl