The PICOCRYPT project, led by the IMDEA Software Institute, will guarantee integrity, privacy and effectiveness of computation on data stored in the cloud

Achieving privacy and integrity in the cloud

Data has emerged as the oil of the 21st century. The importance of data is no longer surprising, but its growing relevance is beginning to take on worrying overtones. Our lives are increasingly dependent on technology that seems to need our data. But where is our data? Where is it stored? Due to the ubiquity of the Internet, everything is now migrated to the cloud.

Zara, Spotify, Netflix, Twitter, practically all companies today use data on which they compute to give us a better service. For example, a music recommendation service should store what we have listened to and cross-reference that data with the data of other people with whom there is a match to try to deduce what else we might like. A financial service could do something similar with investment funds, which is arguably more sensitive information. The same could happen with health data, held by the public health provider or a private company. And all of them, moreover, often have personal information: addresses, email accounts, bank account numbers...

Almost all of these companies rely on external providers for their computing needs: storing data (i.e., delegating its storage) and using it to extract results by running programs on these providers' computers (delegating a computation).

How can we ensure that data and computations that are delegated to third parties are protected against espionage and run correctly? Data can be encrypted, but in order for it to be used by existing software, it needs to be decrypted. At that point, a malicious provider (or a provider that gets hacked) can inspect it and learn data that the company that stored it does not want to disclose and that the person to whom it refers probably does not want to disclose either. Similarly, it could change the program that executes the calculations and return incorrect results, which raises the question of how to check that such results are correct without redoing the computation?

Cryptographic techniques exist to solve both problems. Advancing on them and making them usable in practice is the main objective of the PICOCRYPT project (Cryptography for Privacy and Integrity of Computation on Untrusted Machines), proposed by Dr. Dario Fiore, a researcher at the IMDEA Software Institute of the Madrid Regional Government, which has recently been awarded a Consolidator ERC grant from the European Union (Horizon 2020 research and innovation programme*) to receive funding worth 2 million euros over five years. The European Research Council is the European Union's most prestigious scientific and funding programme. With PICOCRYPT, the IMDEA Software Institute has been granted three projects by this programme (together with RACCOON and MATHADOR).

For Dr. Dario Fiore, cryptography is already a key component to keep our data secure during communication, but "the challenge of PICOCRYPT is to invent new cryptographic protocols to keep our data secure also during computation. The benefits of this paradigm are innumerable. For example, there are people and companies who refrain from using external IT resources because of the risks of this model. With the solutions we intend to design in PICOCRYPT, they could instead use these services securely and without having to fully rely on the providers of these services". It will therefore guarantee the integrity and privacy of computation made with data stored in the cloud and also make it efficient to ensure that delegation is cost-effective.

The IMDEA Software Institute is one of the seven IMDEA Institutes promoted by the Regional Government of Madrid with the aim of carrying out research and scientific development at the highest level.

“This project has received funding from the European Research Council (ERC) under the European Union’s [Horizon 2020 research and innovation programme] (Grant agreement No. [101001283])”

More information:

Blanca Gutiérrez
Communication Manager
IMDEA Software Institute
0034 911 012 202 Ext. 4019 l 0034 680 990 672
blanca.gutierrez@imdea.org