Low-Power encrypted computing solutions

March 4 2022, by Madison Brewer

Smart devices in a flat lay on a white table. Credit: Carnegie Mellon University

Smartphones, smartwatches, smart health devices, and pervasive smart sensors are becoming enmeshed in our daily lives, generating a flood of data that help keep us safe, healthy, and informed. As we see more sources of data, like these low-resource client devices, there is an increasing demand for sophisticated computing on those data, especially to extract value from the data using machine learning. Low-resource devices have limited computing capabilities because of the energy limitation of their small batteries and typically simple computing hardware. To get around these shortcomings, these devices could instead

use computational offloading, sending sensor data for processing to a nearby edge device or to the cloud. Offloading makes even very sophisticated data processing possible, but only with the concession that the server performing the processing has unencrypted access to the data.

A new way of computing, which is called homomorphically encrypted computing, mitigates these privacy concerns: using this technique, the client encrypts its data, sends the encrypted data for offloading, and the offloaded processing happens without ever decrypting the data. Encrypted computing has an extremely high computational cost, which has been mostly regarded as infeasible. Recently, advances in computer architecture and algorithms have made it feasible to offload encrypted computation with reasonable cost, making the technique feasible. However, these advances ignore costs imposed on the low-resource client by encrypted computing, which are associated with arranging the data for encrypted processing, and actually encrypting the data. These costs make encrypted offload computing infeasible for low-resource devices.

McKenzie van der Hagen, a Ph.D. student of electrical and computer engineering at Carnegie Mellon University, and her advisor, Associate Professor Brandon Lucia, have developed new algorithms and hardware designs that directly address these costs to client devices, making encrypted offloading feasible, even for low-resource clients. The two published a paper at this year's annual symposium on Architectural Support for Programming Languages and Operating Systems (ASPLOS). ASPLOS is a venue in the field and is being held in Lausanne, Switzerland from February 28 to March 4.

For encrypted computing, the device encrypts the data such that computations can be performed on it without decrypting it. The drawback, however, is that only linear operations, like addition and multiplication, can be performed on the encrypted data. Research has

traditionally focused on the server because creating work-arounds that fit these constraints drastically increases the number and complexity of computations and thus the time and energy needed.

"The implementations that are available are so highly-optimized for this server that they're not considering the work that has to be done on the client," van der Hagen said. "We show that it's not practical for these resource-constrained clients to participate in these schemes."

Devices that use computational offloading usually send all of the data in one big package and the servers perform lots of computations at once. This requires a lot of energy from the client. Instead, van der Hagen proposes sending the encrypted data in smaller chunks, which would spread the energy demands over a period of time.

Suddenly, multiple rounds of communication with the server becomes feasible. With this new capability, van der Hagen designed processes that are most energy efficient for the client. First, the device collects data, encrypts it, and then sends it to the server. The server performs a handful of linear operations on the encrypted data before sending it back to the device. The device then decrypts the data and completes nonlinear calculations that cannot be done on encrypted data. That data is encrypted again and sent back to the server for another round of linear operations. This process is repeated until the computations are complete.

"We also show that, counterintuitively, it is actually better for the client to be doing this continuous interaction with smaller ciphertexts than to use all of their energy to send a ton of data at the beginning and decrypt a ton of data at the end," van der Hagen said. "We reduce communication costs by up to three orders of magnitude."

This work also introduced new algorithms that make the computations less complex by minimizing the size of the encrypted data, and they

created hardware that supports the use of these algorithms. Both are specially designed for these low power clients. By designing within these constraints, researchers ensure that their work will benefit many devices with a variety of goals.

"The work that we're doing can help clients participate in encrypted computing for many different applications and even applications that are still coming," van der Hagen said. "These are very flexible concepts and flexible implementations that can really help for the future."

More information: The researchers published a paper at this year's annual symposium on Architectural Support for Programming Languages and Operating Systems (ASPLOS).

Provided by Carnegie Mellon University Electrical and Computer Engineering