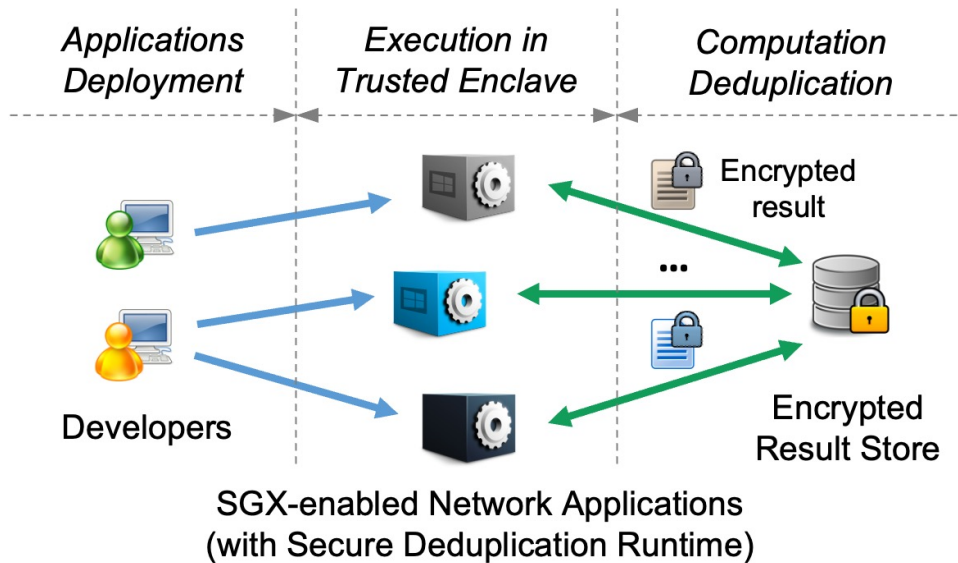# Method for Accelerating Execution of Application in a Trusted Execution Environment

Communications & Information

Computer/AI/Data Processing and Information Technology

Digital Broadcasting, Telecommunication and Optoelectronics

Applications Deployment | **Execution in Trusted Enclave** | **Computation Deduplication**

Encrypted result

Developers

Encrypted Result Store

SGX-enabled Network Applications
(with Secure Deduplication Runtime)

Schematic diagram illustrating a system implementing current invention: Accelerating execution of application in a trusted execution environment.

IP Status
Patent granted

Technology Readiness Level (TRL) ❓   4

Inventor(s)
Prof. WANG Cong
Mr. DUAN Huayi
Dr. CUI Helei
Enquiry: kto@cityu.edu.hk

Opportunity

In response to the wide variety of security risks, researchers have developed hardware-assisted security technologies such as Intel's Software Guard Extensions (SGX). Despite the many promises of this new technology, it is constrained by the limited resources of trusted execution environments (known as enclaves) and the increasingly high workloads that enclaves require. These high workloads can be caused by redundant computations that occur when different applications are handling the same data flows.

This invention provides a secure and generic computation deduplication framework for SGX. The invention allows SGX-enabled applications to identify redundant computations and reuse computation results while also protecting the confidentiality and integrity of the involved code, inputs, and results. The invention also allows multiple applications to securely utilize the shared results of computations. As a result, the invention can greatly increase the performance of Intel SGX.

Technology

This invention is a secure, generic, and developer-friendly software framework that enables hardware-assisted trusted applications to identify redundant computations and reuse computation results, thereby accelerating application processes.

To identify redundant computations, the invention binds a particular computation to its result. Since an enclave is intentionally limited in order to maintain a small trusted computing base (TCB), this invention utilizes an authenticated encryption scheme (AES) to encrypt results and store them outside of the enclave, thereby ensuring the confidentiality and integrity of the stored results.

Moreover, while sharing a system-wide secret key among all applications might be vulnerable to compromise, this invention employs encrypted data (specifically, message-locked encryption) to bind computations and results.

Finally, the invention utilizes a developer-friendly API that allows programmers to deduplicate computations in their SGX-enabled applications with minimal effort.

Advantages

- This invention is the first of its kind to work with hardware-assisted security.
- The invention has a high level of security.
- The invention is developer friendly.

Applications

- Network applications
- Cloud-based executable research platforms (such as Code Ocean)

Develop
Concept

Proof
Concept

Follow-on
Funding

Build Value