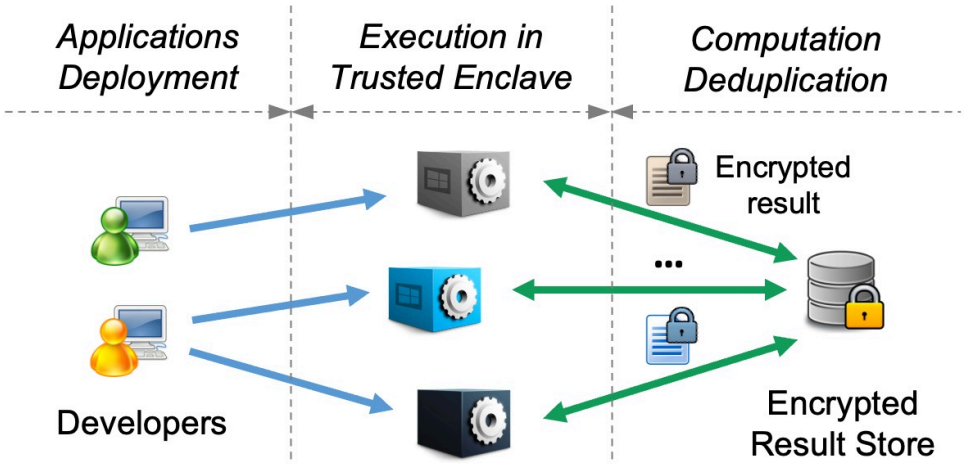
Knowledge Transfer Office
香港城市大學
City University of Hong Kong

加速可信执行环境中应用程序执行的方法

通信和信息

计算机/人工智能/数据处理和信息技术

数字广播、电信和光电



SGX-enabled Network Applications
(with Secure Deduplication Runtime)

IP状态
专利已授权

技术成熟度等级 (TRL) 4

发明人
王聪教授
段华忆
崔禾磊
询问: kto@cityu.edu.hk

本发明是一种安全、通用且对开发者友好的软件框架，能够帮助硬件辅助的可信应用程序识别冗余计算并重复利用计算结果，从而加速应用程序的处理过程。

机会

为了应对各种各样的安全风险，研究人员开发了硬件辅助的安全技术，如英特尔的软件保护扩展（SGX）。尽管这种新技术有很多承诺，但它受限于可信执行环境（称为 enclaves，安全区）的资源有限性，以及 enclaves 所需的日益增加的工作负载。这些高负载可能是由于不同应用程序处理相同数据流时发生的冗余计算所引起的。 本发明提供了一种用于 SGX 的安全通用计算去重框架。本发明允许支持 SGX 的应用程序识别冗余计算并重复利用计算结果，同时保护相关代码、输入和结果的机密性和完整性。本发明还允许多个应用程序安全地共享计算结果。因此，本发明能够大大提高英特尔 SGX 的性能。

技术

本发明是一种安全、通用且对开发者友好的软件框架，能够帮助硬件辅助的可信应用程序识别冗余计算并重复利用计算结果，从而加速应用程序的处理过程。 为了识别冗余计算，本发明将特定的计算与其结果绑定。由于安全区为了保持小型的可信计算基（TCB）而故意有限，本发明使用认证加密方案（AES）来加密结果并将其存储在安全区外，从而确保存储结果的机密性和完整性。此外，虽然在所有应用程序之间共享系统范围的密钥可能存在被泄

露的风险，但本发明采用了加密数据（特别是消息锁定加密）来绑定计算和结果。最后，本发明提供了一个开发者友好的 API，允许程序员在其支持 SGX 的应用程序中以最少的努力去重计算。

优势

- 本发明是首个与硬件辅助安全技术相结合的解决方案
- 本发明具有较高的安全性
- 本发明对开发者友好

应用

- 网络应用程序
- 基于云的可执行研究平台（如 Code Ocean）