Secure IoT Stream Data Management and Analytics with Intel SGX

Swarup Chandra, Vishal M. Karande, and Latifur R. Khan

Department of Computer Science
University of Texas at Dallas, Richardson, TX, USA
{swarup.chandra, vishal.karande, lkhan}@utdallas.edu

Data streams from numerous Internet of Things (IoT) devices, such as medical, home and personal systems, may contain sensitive and confidential information that may need protection against attacks from external adversaries. Beyond addressing challenges in accuracy, space and time, an algorithm designer needs to be aware of perils posed by naive algorithmic implementations under an adversarial setting. Data privacy is threatened mainly due to data sharing.

- IoT devices may communicate with each other for enhanced services. An adversary observing data communication can infer secret information. (E.g., man-in-the-middle attack on data transferred within a compromised home system).
- Since many devices (e.g., personal health monitoring systems) have low hardware resources, data stream analytics may be processed on a third-party server (e.g., a cloud service). An adversary controlling the server may obtain sensitive information.

Though data encryption can conceal sensitive data from an adversary observing data communication, it is challenging to protect data privacy from a more powerful adversary who may have control over the third-party server used for analytics.

Adaptation of generic ORAM (Oblivious RAM) techniques to perform analytics over encrypted data could be computationally

expensive, and would annihilate efforts to reduce training and prediction time. Moreover, privacy-preserving techniques may negatively affect performance (e.g., accuracy). Instead, recent developments in hardware-based trusted computing platforms, such as Intel SGX, can be leveraged for data stream mining when data containing sensitive information is involved. These platforms enable a Trusted Execution Environment (TEE) where code and data are encrypted and can be decrypted within the environment by the CPU. By performing IoT stream analytics within such a trusted computing environment, data privacy and security can be assured to its users. In this talk, we will introduce methods to secure systems that perform data analysis on IoT data streams within a TEE.

Recent studies have shown that a powerful adversary may still be able to infer private information from side channels such as memory access, cache access, CPU usage and other timing channels, thereby threatening data and user privacy. Since a TEE uses shared resources, sensitive information from standard algorithmic design patterns can be inferred by the adversary. The main challenge is to reduce information leak through side-channels and effectively utilize the secure computational environment for IoT data stream analytics. In this talk we will describe a set of techniques that can reduce side-channel information leak while minimizing the computational overhead when performing query processing over IoT data streams.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author.

SafeConfig'17, November 3, 2017, Dallas, TX, USA

© 2017 Copyright is held by the owner/author(s).

ACM ISBN 978-1-4503-5177-5/17/10.

DOI: <https://doi.org/10.1145/3140368.3140377>