SGX-MR: Regulating Dataflows for Protecting Access Patterns of Data-Intensive SGX Applications

AKM Mubashir Alam ¹ Sagar Sharma ² Keke Chen ¹

¹ Trustworthy and Intelligent Computing Lab (TIC), Northwestern Mutual Data Science Institute, Department of Computer Science, Marquette University
² HP Inc.

Introduction

Benefits of cloud computing:
- Economics: pay-as-you-use billing model
- Scalability: plenty of resources for storage and computing
- Accessibility: Easy access regardless of time and location

Security concerns:
- Tamper program
- Tamper data
- Steal sensitive information

Goal:
- Confidentiality: Server learns nothing about user program and data
- Integrity: Server execute desired program and return accurate result
- Efficiency: Faster execution time

Existing Solutions

- Software-based crypto approaches such as Fully Homomorphic Encryption (FHE), Secure Multi-party Computation (SMC), etc. address the confidentiality problem. But they are too expensive to be practical.
- Trusted Execution Environment (TEE) overcomes the performance issue. Provides confidentiality assurance by applying hardware encryption and isolated execution that enables plain text computation.

We propose SGX-MR
- A framework that regulates the dataflow of SGX applications utilizing MapReduce
- Covers a wide range of applications
- Data Mining
- Text Processing
- Machine Learning
- Basic Statistics etc.

Design

- Framework divides into two parts
- Untrusted component contains a small initiator program
- encrypted files and data blocks
- Enclave holds the rest
- MR Controller manages the data flow
- Only access equal size blocks
- User define functions execute in Enclave
- Mapper
- Reducer

Our Observation

ORAM incurs high computation cost
- Regulating data flow can be more efficient than ORAM primitive
- Some Application Specific Access Pattern does not leak additional information
- Other access patterns can be replaced with specific Oblivious Algorithm

Challenges
- Application specific analysis
- Time Consuming
- Error Prone

Evaluate SGX-MR

- mitigates intermediate access patterns
- Synergy of SGX-MR’s curtailed components (e.g., combiner, oblivious sort, and reducer) efficiently hides the access pattern leakages

Conclusion

- SGX-MR avoids (1) expensive ORAM as block I/O and (2) error-prone application-specific design of access pattern protection
- It uses MapReduce to regulate application dataflows – protects a large class of data-intensive applications
- It addresses both access-pattern attacks and page-fault attacks