SecDATAVIEW: A Secure Big Data Workflow Management System for Heterogeneous Computing Environments

Saeid Mofrad, Ishtiaq Ahmed, Shiyong Lu, Ping Yang, Heming Cui, Fengwei Zhang*
{saeid.mofrad, ishtiaq, shiyong, fengwei}@wayne.edu
pyang@binghamton.edu
heming@cs.hku.hk

*The corresponding author, and he is currently affiliated with SUSTech.
Outline

- Introduction
- x86 TEE technology background
- Previous data analytics systems with TEE support
- SecDATAVIEW
- Performance results and security comparison
- Conclusions and future work
Outline

➢ Introduction
➢ x86 TEE technology background
➢ Previous data analytics systems with TEE support
➢ SecDATAVIEW
➢ Performance results and security comparison
➢ Conclusions and future work
Cloud Platform for Big Data Analytics

➢ Cloud platforms are common for big data analytics

➢ Isolation through software virtualization is used to achieve trusted execution environment (TEE) in cloud infrastructure

➢ **Downsides of virtualization [3]:**

1) Virtualization uses shared hardware, hypervisor and cloud system software thus increases the software and hardware TCB of the cloud platform

2) Hypervisor and cloud’s system software contain thousands of lines of code and may have security flaws

3) Many hypervisor exploits have been reported in clouds [5,6]

4) Increased TCB size means less security
Outline

➢ Introduction

➢ x86 TEE technology background

➢ Previous data analytics systems with TEE support

➢ SecDATAVIEW

➢ Performance results and security comparison

➢ Conclusions and future work
Hardware-Assisted Trusted Execution Environment in x86 Architecture [3]

- Hardware-Assisted TEE couples hardware with TEE abstraction so mitigates the downsides of the software only TEEs
- Hardware-Assisted TEE may be faster since it uses dedicated hardware
- Hardware-Assisted TEE exposes small size of hardware TCB and smaller TCB means better security
- “Older” Hardware-Assisted TEE: Intel ME, AMD PSP, and x86 SMM [4]

- Two general-purpose Hardware-Assisted TEE in x86 architecture:
  1. Intel Software Guard eXtensions (SGX) [HASP 2013], [1]
Background: Intel SGX and AMD SEV [3]
## Intel SGX VS AMD SEV [3]

<table>
<thead>
<tr>
<th>TEE Technology</th>
<th>Runtime Access Privilege</th>
<th>Memory Size Limits</th>
<th>SDK</th>
<th>Software Change</th>
<th>Platform Attestation Mechanism</th>
<th>TEE Protection guarantee</th>
<th>TEE TCB SIZE</th>
<th>TEE performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel SGX</td>
<td>Ring 3</td>
<td>Up to 128MB</td>
<td>Provided</td>
<td>Required</td>
<td>Attested through Intel remote attestation</td>
<td>Confidentiality and Integrity protection of the enclave’s code and data at runtime</td>
<td>Smaller than SEV</td>
<td>Performs slower than SEV</td>
</tr>
<tr>
<td>AMD SEV</td>
<td>Ring 0</td>
<td>Up to available system memory</td>
<td>Not Required</td>
<td>Not required</td>
<td>Attested through AMD guest attestation</td>
<td>Confidentiality protection of the VM’s memory image at runtime</td>
<td>Larger than SGX</td>
<td>Performs faster than SGX</td>
</tr>
</tbody>
</table>
Outline

- Introduction
- X86 TEE technology background
- Previous data analytics systems with TEE support
- SecDATAVIEW
- Performance results and security comparison
- Conclusions and future work
Previous Data Analytics Systems with TEE Support

➢ VC3: A trustworthy Hadoop based data analytics platform in the cloud that leverages SGX to protect unmodified Map-Reduce tasks written in C/C++ [S&P 2015], [7]

➢ A lightweight, Map-Reduce framework with Lua, a high-level language that interprets the Map-Reduce Lua scripts in Intel SGX [CCGRID 2017], [8]

➢ Opaque: An oblivious and encrypted distributed analytics platform that enhanced the security of the Spark SQL with SGX [NSDI 2017], [9]

❖ Shortcomings with previous data analytics platforms with TEE support:

1. **Limited functionality**: They only support Map/Reduce or SQL query data types

2. **Lack of support for heterogeneous cloud infrastructure**: They only support Intel SGX platform
Outline

➢ Introduction
➢ X86 TEE technology background
➢ Previous data analytics systems with TEE support
➢ SecDATAVIEW
➢ Performance results and security comparison
➢ Conclusions and future work
SecDATAVIEW: A Secure Data Analytics System with Heterogeneous TEE Support

SecDATAVIEW main characteristics:

- **Different data types:**
  1. Supports scientific big data workflow [10] and considers each task as a black box
  2. Supports many type of workflows (Map-Reduce, Query, Machine learning, Deep learning, Image-Video processing, etc.)

- **Heterogeneous TEE:**
  1. Supports both Intel SGX and AMD SEV at the same time

- **Strong security guarantee:**
  1. Protects the confidentiality and integrity of code and data for workflows running on public untrusted clouds
  2. Supports High-level and managed code programming language (Java) that protects memory leaks vulnerability (buffer overflow)
  3. Provides minimal hardware and software TCB for general purpose cloud based big data analytics platform

- **Flexible system settings (SGX mode, SEV mode, Hybrid mode) for enhanced security and performance requirements:**
  1. Supports trade-off between enhanced security (SGX mode) and performance (SEV mode) for workflows with different user requirements.
SecDATAVIEW: Leverages Heterogenous Workers with TEE Support

- **SecDATAVIEW Intel SGX Worker:**
  1. Uses SGX shield [19] programming model
  2. SGX-LKL [20] is incorporated to provide the Java virtual machine in the SGX enclave
  3. Encrypted SGX-LKL disk image is used to protect the confidentiality of user code and data at rest
  4. Java reflection and class loader are incorporated to overcome lack of multi-process support in the SGX-LKL

- **SecDATAVIEW AMD Worker:**
  1. Uses AMD Secure Encrypted Virtualization (SEV)
  2. SEV-protected VM is used to protect the worker memory image at runtime
  3. Java virtual machine is used in every SEV-protected VM
SecDATAVIEW: Adversary Model

- SecDATAVIEW threat model targeted attacks that happen on untrusted cloud:
  1) Attacks that exploit flaws or vulnerabilities in the hypervisor, or cloud’s system software layer trying to gain access to the user data or results stored on unprotected memory
  2) Attacks that could happen by dishonest administrator to gain access to data or results stored on the user storage medium

- Attacks, including network traffic-analysis [11], denial-of-service, access pattern leakage [12], side-channels [13], and fault injections [14], are out of the scope
SecDATAVIEW System Architecture
WCPAC: Workflow Code Provisioning and Communication Protocol

The WCPAC protocol’s main functionality includes:

1. to provision and attest secure worker nodes
2. to provision securely the code for the Task Executor and workflow tasks on each participating worker node
3. to establish the secure communication and file transfers between the master node and worker nodes
4. to ensure secure file transfers among worker nodes
WCPAC: Workflow Code Provisioning and Communication Protocol
WCPAC: Workflow Code Provisioning and Communication Protocol
WCPAC: Workflow Code Provisioning and Communication Protocol
WCPAC: Workflow Code Provisioning and Communication Protocol

[Diagram of workflow code provision and communication protocol]
WCPAC: Workflow Code Provisioning and Communication Protocol
WCPAC: Workflow Code Provisioning and Communication Protocol
WCPAC: Workflow Code Provisioning and Communication Protocol
WCPAC: Workflow Code Provisioning and Communication Protocol
WCPAC: Workflow Code Provisioning and Communication Protocol
WCPAC: Workflow Code Provisioning and Communication Protocol
Outline

➢ Introduction

➢ X86 TEE technology background

➢ Previous data analytics systems with TEE support

➢ SecDATAVIEW

➢ Performance results and security comparison

➢ Conclusions and future work
# Testbeds Configuration

<table>
<thead>
<tr>
<th>Testbed Machine</th>
<th>SecDATAVIEW Master</th>
<th>Intel Worker</th>
<th>AMD Worker</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Model</td>
<td>Intel Core i7-6700T</td>
<td>Intel Xeon E3-1275 v5</td>
<td>EPYC-7251</td>
</tr>
<tr>
<td>Motherboard</td>
<td>Dell Inspiron 24-5459</td>
<td>Intel FOG</td>
<td>GIGABYTE MZ31-AR0</td>
</tr>
<tr>
<td>Memory</td>
<td>12GB DDR4 Non-ECC</td>
<td>32GB DDR4 No-ECC</td>
<td>32GB DDR4-ECC</td>
</tr>
<tr>
<td>Storage</td>
<td>Conventional HDD</td>
<td>NVME SSD</td>
<td>SATA SSD</td>
</tr>
<tr>
<td>Operating System</td>
<td>Linux 16.04 LTS</td>
<td>Linux 16.04 LTS</td>
<td>Ubuntu 18.04 LTS</td>
</tr>
<tr>
<td>OS, Hypervisor kernel</td>
<td>4.15.0-50-generic-x64</td>
<td>4.15.0-50-generic x64</td>
<td>4.20.0-sev-x64</td>
</tr>
<tr>
<td>TEE SDK Version</td>
<td>N/A</td>
<td>SGX SDK Ver 2.00</td>
<td>N/A</td>
</tr>
<tr>
<td>SGX-LKL</td>
<td>N/A</td>
<td>Hardware Mode</td>
<td>N/A</td>
</tr>
<tr>
<td>SGX-LKL Memory</td>
<td>N/A</td>
<td>2GB (Encrypted)</td>
<td>N/A</td>
</tr>
<tr>
<td>SGX-LKL Storage</td>
<td>N/A</td>
<td>2GB (Encrypted Disk Image)</td>
<td>N/A</td>
</tr>
<tr>
<td>SEV VM Kernel</td>
<td>N/A</td>
<td>N/A</td>
<td>4.18.20-generic-x64</td>
</tr>
<tr>
<td>SEV VM Memory</td>
<td>N/A</td>
<td>N/A</td>
<td>4GB (Encrypted)</td>
</tr>
<tr>
<td>SEV VM Storage</td>
<td>N/A</td>
<td>N/A</td>
<td>32GB (Disk Image)</td>
</tr>
</tbody>
</table>
The Diagnosis Recommendation Workflow [15]

- SGX mode overhead 2.62x
- SEV mode overhead 1.29x
- Hybrid mode overhead 1.20x
- Hybrid mode used two SGX and two SEV workers.
The Word Count (Map-Reduce) workflow [16]

- SGX mode overhead 1.89x
- SEV mode overhead 1.04x
- Hybrid mode overhead 1.33x
- Hybrid mode used two SGX and two SEV workers
The Distributed K-means workflow [17]

- SGX mode overhead 1.69x
- SEV mode overhead 1.29x
- Hybrid mode overhead 1.43x
- Hybrid mode used two SGX and two SEV workers
SecDATAVIEW: Security and TCB Analysis

- **SecDATAVIEW Intel SGX Worker:**
  - The software TCB is the LibOS, the JVM, the Code Provisioner, and the Task Executor
  - The hardware TCB is the CPU package for the SGX workers

- **SecDATAVIEW AMD Worker:**
  - The software TCB is the guest OS, the JVM, the Code Provisioner, and the Task Executor
  - The hardware TCB is AMD SoC and AMD secure processor for the SEV worker nodes

- SecDATAVIEW is protected against memory corruption vulnerabilities (Java)
- Workflow runtime is protected with hardware-assisted TEE
- Network traffic is protected with SSL protocol
- User data and results are protected with AES GCM-256 AEAD cryptography scheme
## Functional Comparison with Existing Systems

<table>
<thead>
<tr>
<th>Feature</th>
<th>SecDATAVIEW</th>
<th>VC3</th>
<th>Opaque</th>
<th>Lua Map/Reduce</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data confidentiality</strong></td>
<td>AES-GCM-256</td>
<td>AES-GCM-128</td>
<td>AES-GCM-128</td>
<td>AES-CTR-128</td>
</tr>
<tr>
<td><strong>Data integrity</strong></td>
<td>Authenticated Encryption</td>
<td>Authenticated Encryption</td>
<td>Authenticated Encryption</td>
<td>No</td>
</tr>
<tr>
<td><strong>Intel SGX</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>AMD SEV</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Data structure compatibility</strong></td>
<td>All types of workflow</td>
<td>Map-Reduce</td>
<td>SQL query</td>
<td>Map-Reduce</td>
</tr>
<tr>
<td><strong>Job integrity verification</strong></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Access pattern leakage protection</strong></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Access pattern leakage overhead</strong></td>
<td>N/A</td>
<td>N/A</td>
<td>1.6X-46X (oblivious mode)</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Job performance overhead</strong></td>
<td>1.2X-1.43X (hybrid mode)</td>
<td>1.04X-1.08X (base-encrypted mode)</td>
<td>0.52X-3.3X (encrypted mode)</td>
<td>1.3X-2X (encrypted mode)</td>
</tr>
</tbody>
</table>
Outline

➢ Introduction
➢ X86 TEE technology background
➢ Previous data analytics systems with TEE support
➢ SecDATAVIEW
➢ Performance results and security comparison
➢ Conclusions and future work
Conclusions and Future Work

➢ SecDATAVIEW, is an efficient and secure big data workflow management system that protects the confidentiality and integrity of Java-written tasks and data in the workflow with the help of SGX/SEV worker nodes.

➢ SecDATAVIEW significantly reduces the TCB size of the worker node and protects the Task Executor and individual workflow tasks by executing them inside the SGX enclave or the SEV-protected instance.

➢ Our experiments with different types of workflows show the usability of the system with a low-performance overhead while securing the confidential task execution at SGX enclave/SEV instance runtime.

➢ Future work: Investigate the security issues of collaborative scientific workflows [17]
References


References Continue


[18] https://www.flickr.com/photos/waynestateise/47529826741/


Thank You!

Email: saeid.mofrad@wayne.edu

The first release of SecDATAVIEW is available at

https://github.com/shiyonglu/SecDATAVIEW

Artifacts Evaluated – Functional