SETU

Ollscoil
Teicneolaíochta
an Oirdheiscirt

South East
Technological
University

A Detailed Study on Confidential Computing

By
Syed Muhammad Umar
C00278724@setu.ie
Lecturer: Lei Shi

Date: 18/05/2025

Table of Contents

Introduction

With rapid advancements in Artificial Intelligence (AI) and Machine Learning (ML), organizations now generate and process vast volumes of data every second. As the saying goes, “With great power comes great responsibility,” and safeguarding this data has become a critical obligation.

In computing, data typically exists in three states [1]: in transit (while being transmitted across networks), at rest (when stored on physical or cloud storage), and in use (while actively being processed by CPUs and memory).

Current encryption technologies effectively protect data at rest and in transit. However, data in use remains vulnerable, as it must be decrypted during processing — exposing it to potential threats such as side-channel attacks and malicious insiders. This creates a significant security gap in modern computing environments, especially in public and multi-tenant cloud infrastructures.

Problem Statement: Securing Data in Use

Traditional security measures fail to fully protect data while it is being processed in memory. Unlike data at rest or in transit, which can remain encrypted, data in use typically must be decrypted for operations—making it visible and exploitable.

The rise of cloud computing, multi-tenant environments, and remote data processing amplifies this vulnerability. These challenges demand a new approach that ensures data remains protected even during computation.

Confidential Computing: A New Paradigm

To address the challenge of securing data during active processing, Confidential Computing has emerged as a transformative solution. It safeguards data in use by performing computations within a hardware-based, attested Trusted Execution Environment (TEE).

These secure and isolated environments ensure that applications and data remain shielded from unauthorized access or tampering during runtime. By minimizing exposure during processing, Confidential Computing significantly enhances data security—especially for organizations managing sensitive, regulated, or mission-critical information in the cloud.

Technologies Enabling Confidential Computing

Intel® Software Guard Extensions (SGX)

Intel® SGX is one of the foundational technologies enabling Confidential Computing.[2] It allows application developers to protect sensitive code and data from unauthorized access or modification by using secure, isolated regions of memory called enclaves.

These enclaves ensure that even if the operating system, BIOS, virtual machine monitor, or drivers are compromised, the data inside remains secure. SGX relies on hardware-based memory protection mechanisms to guard against threats such as memory snooping, tampering, and cold boot attacks.

The Intel SGX SDK (available for Linux OS) provides developers with a set of APIs, libraries, tools, and sample code to build secure applications using C/C++. Applications can utilize SGX instructions introduced with Intel’s 6th generation Core™ processors or newer.

Key advantages of Intel SGX include:

- Secure enclave execution isolated from the rest of the system
- Protection against privileged system-level attacks
- Minimal trusted computing base (TCB)
- Support for remote attestation, allowing validation of enclave integrity
- Compatibility with standard development workflows

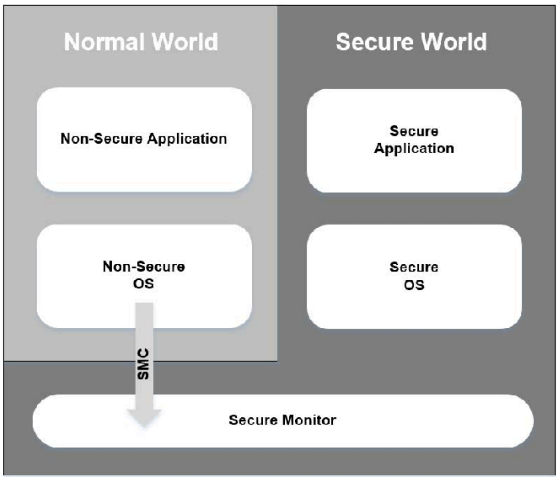
Arm Trustzone

Arm TrustZone is a hardware-based security extension integrated into Arm's Cortex-A processors, designed to establish a Trusted Execution Environment (TEE). This [3] technology partitions the system into two distinct worlds: the Secure World and the Normal World. The Secure World handles sensitive operations such as trusted boot processes, cryptographic functions, and digital rights management (DRM), while the Normal World runs the standard operating system and applications.

A key feature of TrustZone is its ability to isolate sensitive code and data from the rest of the system, ensuring that even if the Normal World is compromised, the Secure World remains protected. This isolation is enforced by hardware, preventing unauthorized access to secure resources. The transition between these worlds is managed by a component known as the Secure Monitor, which controls the context switching and maintains the integrity of the Secure World.

TrustZone's flexibility allows system-on-chip (SoC) designers to tailor security implementations to specific needs, making it a foundational technology for various applications, including mobile device management, secure payments, and confidential data processing in cloud environments.

By providing a robust framework for secure execution, Arm TrustZone plays a pivotal role in enhancing the security posture of modern computing systems, particularly in scenarios where protecting data in use is critical.



AMD Secure Encrypted Virtualization (SEV)

AMD Secure Encrypted Virtualization (SEV) [4] is a hardware-based security feature designed to protect virtual machines (VMs) by encrypting their memory, ensuring that data remains confidential even in multi-tenant cloud environments. By integrating memory encryption capabilities with AMD's virtualization architecture, SEV allows each VM's memory to be encrypted with a unique key managed by the AMD Secure Processor. This isolation ensures that even if the hypervisor or other VMs are compromised, the data within a protected VM remains secure

Key Features:

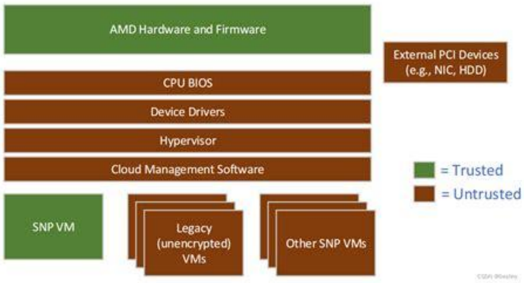
- Memory Encryption: Each VM's memory is encrypted using a unique key, preventing unauthorized access from other VMs or the hypervisor.
- Transparent Operation: SEV operates without requiring modifications to applications,

making it easier to deploy in existing environments.
- Enhanced Isolation: By encrypting the memory, SEV provides strong isolation between VMs, enhancing security in shared environments.

Advanced Extensions:

- SEV-ES (Encrypted State): Extends SEV by encrypting the CPU register state of VMs, protecting against attacks that target CPU registers during context switches.
- SEV-SNP (Secure Nested Paging): Further enhances security by adding memory integrity protection, preventing malicious modifications to VM memory and defending against certain types of attacks from compromised hypervisors.

By leveraging SEV and its extensions, organizations can enhance the confidentiality and integrity of their workloads in virtualized and cloud environments, aligning with the principles of Confidential Computing.

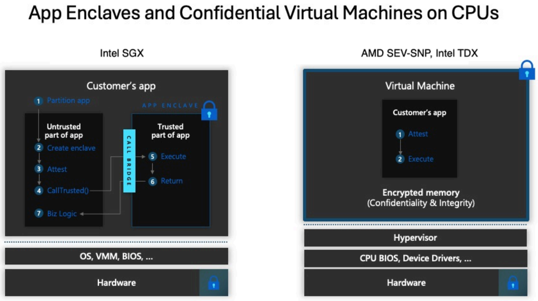


TEE on Cloud

A TEE is a hardware-enforced, isolated area within a processor that ensures code and data loaded inside are protected with respect to confidentiality and integrity. In cloud computing, TEEs safeguard data in use by: [5]

- Isolation: Ensuring that data and code within the TEE are inaccessible to the rest of the system, including the operating system, hypervisor, and even cloud service providers.
- Integrity: Allowing only authorized code to execute within the TEE, preventing unauthorized modifications.
- Confidentiality: Encrypting data within the TEE, so that even if the system is compromised, the data remains secure.

Azure implements TEEs using technologies like Intel SGX and AMD SEV-SNP, enabling customers to run sensitive workloads with enhanced security. These TEEs support remote attestation, allowing verification that the code inside the TEE is trustworthy before processing sensitive data.



Real World Application

Confidential AI and Machine Learning

Confidential Computing allows for the training and deployment of AI/ML models on sensitive data within Trusted Execution Environments (TEEs). This ensures that proprietary algorithms and datasets remain protected during processing. [6] Industries handling confidential information, such as healthcare and finance, can leverage this to maintain data privacy while harnessing AI capabilities.

Privacy-Preserving Analytics

With Confidential Computing, organizations can perform analytics on encrypted data without decrypting it, maintaining data confidentiality. This is crucial for businesses that need to analyze sensitive information, like user behavior or financial transactions, while adhering to privacy regulations.

Enhanced Data Protection in Healthcare

Healthcare providers can utilize Confidential Computing to process patient data securely, ensuring compliance with regulations like HIPAA. This enables secure sharing and analysis of medical records, facilitating research and improving patient care without compromising privacy.

Strengthened Security for Financial Services

Financial institutions can process sensitive transactions and customer data within TEEs, reducing the risk of data breaches. Confidential Computing helps in safeguarding against insider threats and ensures compliance with stringent financial regulations.

Cloud Platforms Providing Confidential Computing Services

Common Features Across Providers

Before detailing each provider, mention that many Confidential Computing services share a common foundation:

Most major cloud platforms—such as Microsoft Azure, Google Cloud, and Amazon Web Services—implement Confidential Computing using TEEs that provide:

- **Memory Encryption**: Keeps data encrypted while in use.
- **Hardware-Based Isolation**: Prevents access by hypervisors, OS, or cloud operators.
- **Remote Attestation**: Verifies the integrity of the environment before code execution.
- **Integration with Cloud Services**: Supports secure deployment of containers, analytics, and AI workloads.
- **Support for GPUs**: Extends TEEs to GPU processing for machine learning and analytics.

Microsoft Azure

- Offers **Confidential VMs** using AMD SEV-SNP and Intel TDX.
- Provides **virtual TPM**, **OS disk encryption**, and multiple VM series (e.g., DCasv5, ECesv5).
- Suitable for both general-purpose and GPU-heavy workloads [7].

Google Cloud

- Offers **Confidential VMs** with integration into **Confidential GKE Nodes** and **Dataproc**.
- Unique offering of **Confidential AI support with NVIDIA H100 GPUs**.
- Strong use cases in **secure multi-party data analytics** [8].

Amazon Web Services (AWS)

- Offers **AWS Nitro Enclaves** instead of full Confidential VMs.
- Focused on isolating and securely processing highly sensitive data without network access [9].

Pros and Cons

Advantages

Confidential Computing offers significant advantages in securing sensitive data during processing. It ensures **enhanced data protection** by keeping data encrypted even while in use, thereby reducing the risk of breaches. It also delivers strong **privacy assurance**, as data is processed within secure, isolated environments, safeguarding it from unauthorized access — even in **untrusted infrastructures** like public cloud or third-party servers.

Additionally, it helps protect **intellectual property**, allowing organizations to run proprietary algorithms and handle confidential data without exposing code or logic. Finally, Confidential Computing supports **regulatory compliance** by providing a secure processing framework that aligns with privacy and data protection laws.

Disadvantages

Despite its security benefits, Confidential Computing comes with several challenges. It may introduce **performance overhead** due to the additional processing required for encryption and isolation, potentially slowing down applications. The technology also adds **complexity and cost**, as it often requires specialized hardware, software, and expertise to implement effectively.

Another limitation is its **limited adoption**—as the technology is still emerging, it may not be fully compatible with existing systems or widely supported across all platforms. Additionally, there is a **risk of misuse**; if not properly managed, the secure environments could be exploited to hide malicious activity, emphasizing the need for strong oversight and security controls.

Conclusion

In an era where data security and privacy are more critical than ever, **Confidential Computing** emerges as a groundbreaking solution for protecting data in its most vulnerable state—**while in use**. By leveraging **Trusted Execution Environments (TEEs)** and hardware-based isolation, it ensures that sensitive data remains encrypted and shielded even during processing. This innovation enables secure computing in untrusted environments, supports privacy-preserving collaboration, and helps organizations meet stringent **regulatory compliance** requirements.

However, the adoption of Confidential Computing is not without challenges. Organizations must navigate **performance overhead**, **implementation complexity**, and the **need for specialized infrastructure**. Additionally, as the technology evolves, there must be careful consideration to prevent **potential misuse** and to ensure interoperability with existing systems.

Despite these limitations, the benefits of enhanced security, **intellectual property protection**, and **data privacy assurance** make Confidential Computing a vital tool in the modern cloud computing landscape.

As adoption increases and technology matures, it is poised to become a standard for secure computing across industries.

References

1. Confidential Computing Consortium (2022) *CCC Outreach White Paper* (Updated November 2022). Available at: https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/CCC_outreach_whitepaper_updated_November_2022.pdf (Accessed: 18 May 2025).

2. Intel Corporation (n.d.) *Intel® Software Guard Extensions SDK for Linux OS*. Available at: https://www.intel.com/content/www/us/en/developer/tools/software-guard-extensions/linux-overview.html (Accessed: 18 May 2025).

3. Arm Ltd. (n.d.) *Arm TrustZone for Cortex-A*. Available at: https://www.arm.com/technologies/trustzone-for-cortex-a (Accessed: 18 May 2025).

4. AMD (n.d.) *Secure Encrypted Virtualization (SEV)*. Available at: https://www.amd.com/en/developer/sev.html (Accessed: 17 May 2025).

5. Microsoft (n.d.) *Trusted Execution Environment in Azure Confidential Computing*. Available at: https://learn.microsoft.com/en-us/azure/confidential-computing/trusted-execution-environment (Accessed: 17 May 2025).

6. Google Cloud (n.d.) *Confidential Computing for Analytics and AI*. Available at: https://cloud.google.com/architecture/confidential-computing-analytics-ai (Accessed: 17 May 2025).

7. Microsoft (n.d.) *Azure Confidential Virtual Machines Overview*. Available at: https://learn.microsoft.com/en-us/azure/confidential-computing/confidential-vm-overview (Accessed: 17 May 2025).

8. Google Cloud (n.d.) *Confidential Virtual Machines Overview*. Available at: https://cloud.google.com/confidential-computing/confidential-vm/docs/confidential-vm-overview (Accessed: 17 May 2025).

9. Amazon Web Services (n.d.) *AWS Confidential Computing*. Available at: https://aws.amazon.com/confidential-computing/ (Accessed: 17 May 2025).