Global Research Journal in Engineering, Science, Technology and Management (GRJESTM)
Volume 02, Issue 03 (May-June) 2026, pp. 376-380
GRJESTM :: An odaswa™ Journal
ISSN : 3107-3611 (Online)

TECHNICAL SERIES | TECHNOLOGY INSIGHT – TN10

Confidential Computing: Protecting Data During Processing through Trusted Execution Environments

Ravi K Prasad[1]* and Shalini K[2]

Technology Snapshot.

Technology Domain	Cybersecurity and Computer Architecture
Core Technologies	Trusted Execution Environments, memory encryption, remote attestation and hardware-based isolation
Major implementations	Intel SGX, Intel TDX, AMD SEV-SNP and Arm Confidential Computing Architecture
Primary Applications	Cloud security, healthcare, financial services, confidential AI and privacy-preserving analytics
Key Advantages	Protection of sensitive data during computation, workload isolation and verifiable execution environments
Key Challenges	Side-channel attacks, performance overhead, platform compatibility and trust management

Keywords: Confidential Computing, Trusted Execution Environment, TEE, Remote Attestation, Memory Encryption, Hardware Security, Cloud Security.

* 1. Department of Computer Science and Engineering, Amity University, Noida, Uttar Pradesh, India.
2. Department of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India.

Copyright: © 2026 Ravi K Prasad and Shalini K. This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited. Published By **odaswa**. Published in Chennai, Tamil Nadu, India

1. Introduction

Modern computing environments increasingly depend on cloud infrastructure, distributed applications and shared processing platforms. Conventional security mechanisms protect information through encryption when it is stored or transmitted. However, sensitive information may become exposed when it is loaded into memory and processed by applications. During this stage, privileged software components, including operating systems and hypervisors, may potentially access application data.

Confidential Computing addresses this security gap by protecting data while it is being processed. The Confidential Computing Consortium (CCC) defines the technology as the protection of data in use through computation inside a hardware-based, attested Trusted Execution Environment (TEE) [1].

A TEE establishes an isolated execution environment in which selected application code and associated data are protected from unauthorized access or modification. Hardware security mechanisms enforce the isolation, while remote attestation enables an external party to verify the security configuration before sensitive information is supplied.

This approach is particularly relevant to cloud computing, where organizations may need to process confidential information on infrastructure that they do not physically own or directly administer.

2. Technical Background

Data security is generally considered across three states: data at rest, data in transit and data in use. Encryption at rest protects information stored in databases, files and storage systems. Transport Layer Security (TLS) protects information during network communication. However, conventional encryption alone does not fully address the exposure that occurs when applications process information in memory.

Confidential Computing introduces hardware-supported isolation to protect sensitive workloads during execution. A TEE separates protected application execution from the surrounding software environment. Depending on the architecture, this isolation may be provided at the process level or across an entire virtual machine.

A major concept associated with TEEs is the Trusted Computing Base (TCB). The TCB consists of the hardware, firmware and software components that must function correctly to maintain the intended security properties. Reducing the size and complexity of the TCB is important because vulnerabilities in trusted components can compromise the protected environment.

Confidential Computing therefore combines hardware security features, secure initialization, memory protection, cryptographic verification and controlled application execution. It complements rather than replaces conventional encryption and access-control mechanisms [2].

3. Trusted Execution Environment and Operating Principle

A graph-based RAG workflow generally consists of the following stages.

A Trusted Execution Environment is an isolated processing area designed to protect the confidentiality and integrity of code and data. It establishes a security boundary between the protected workload and other components of the computing platform.

The operating principle involves the following stages.

Stage 1: Secure workload initialization. The application and its required components are loaded into the protected execution environment. Hardware mechanisms establish the isolation boundary and protect the workload's memory.

Stage 2: Code and configuration measurement. The platform generates cryptographic measurements representing relevant software and configuration components.

These measurements help identify the workload and its execution environment.

Stage 3: Remote attestation. A remote verifier examines cryptographically protected evidence generated by the platform. It checks whether the hardware and software configuration satisfy predefined security policies. Attestation provides a basis for deciding whether the environment should be trusted [3].

Stage 4: Secure data provisioning. After successful verification, sensitive data and cryptographic keys can be delivered through an authenticated and protected communication channel to the approved execution environment.

Stage 5: Protected computation. The application processes the supplied information within the TEE. Hardware-supported isolation and memory protection help prevent unauthorized access from other software components.

Stage 6: Controlled output. The application returns authorized results to the requesting system. Output policies may restrict the disclosure of sensitive intermediate information.

An important distinction is that memory encryption does not mean that data remain encrypted in the exact same form throughout every processor operation. The hardware protects memory and access boundaries, while the processor performs authorized computation on the data inside the protected environment.

4. Major Confidential Computing Architectures

Several processor architectures provide hardware support for confidential computing.

- **Intel Software Guard Extensions (SGX):** Intel SGX provides process-level isolation through protected memory regions known as enclaves. Selected application code and data execute inside these enclaves, limiting access by the operating system and other applications. This architecture offers a relatively small isolation boundary but may require application modification and careful management of interactions with the untrusted operating system.
- **Intel Trust Domain Extensions (TDX):** Intel TDX provides hardware-assisted isolation for confidential virtual machines, known as Trust Domains. It is designed to protect virtual-machine memory and execution state from certain privileged software components, including the hypervisor.
- **AMD Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP):** AMD SEV-SNP extends virtual-machine memory encryption with additional integrity and memory-management protections. It helps isolate confidential virtual machines from the hypervisor and other virtual machines, subject to the platform's security model.
- **Arm Confidential Computing Architecture (CCA):** Arm CCA introduces hardware-supported isolation through protected execution environments known as Realms. It is designed to protect workloads from the normal operating system and other software components, including privileged software in the conventional execution environment.

These architectures differ in isolation granularity, memory protection mechanisms, application compatibility and attestation procedures. The appropriate implementation depends on workload requirements and the platform's security assumptions.

5. Applications of Confidential Computing

Confidential Computing is increasingly relevant to applications that require sensitive information to be processed outside the direct control of its owner.

Healthcare data processing: Hospitals and research organizations can use protected execution environments to analyse medical datasets while reducing the exposure of patient

information to underlying infrastructure operators.

Financial services: Banks and financial institutions can use confidential environments for transaction processing, fraud detection and risk analysis involving confidential customer and business information.

Cloud computing: Organizations can deploy sensitive applications on third-party cloud infrastructure while using hardware-backed isolation and attestation to establish additional security assurance.

Artificial intelligence: Confidential Computing can help protect AI model parameters, inference inputs and sensitive datasets during processing. This is particularly relevant when organizations use external infrastructure to execute AI workloads.

Collaborative data analytics: Multiple organizations may wish to analyse combined datasets without granting one another direct access to the underlying confidential information. Confidential execution environments can support such controlled processing arrangements.

Edge computing: Devices deployed in remote or physically accessible locations can use hardware-supported isolation to protect sensitive application data and execution processes.

6. Security Challenges and Limitations

Although TEEs strengthen data protection, they do not eliminate all cybersecurity risks.

Side-channel attacks: Attackers may infer sensitive information through indirect observations such as memory access patterns, cache behaviour, execution timing or other shared hardware resources. Hardware isolation does not automatically prevent every side-channel attack.

Implementation vulnerabilities: Programming errors, insecure interfaces and weaknesses in trusted application code can expose protected information. A TEE cannot compensate for every software vulnerability.

Attestation and trust management: Remote attestation depends on trustworthy hardware roots, cryptographic evidence, verification services and appropriate security policies. Compromise of these components can undermine the trust process.

Performance overhead: Memory encryption, integrity checking, secure context switching and communication between protected and unprotected environments may introduce additional processing costs. The impact depends on workload characteristics and architecture.

Platform compatibility: Different processor vendors implement TEEs using different architectures and interfaces. This creates challenges for application portability, software development and interoperability.

Availability and operational risks: Confidential Computing primarily addresses confidentiality and integrity. It does not independently guarantee service availability, prevent denial-of-service attacks or protect every external system connected to a workload.

Consequently, TEEs should be deployed as one layer within a broader security architecture that includes secure software development, access controls, network protection, monitoring and vulnerability management.

7. Emerging Directions and Future Outlook

Confidential Computing is moving beyond isolated application enclaves toward confidential virtual machines, containers and heterogeneous computing environments. This development is intended to support larger workloads while reducing the application changes required for deployment.

Another important direction is the protection of artificial intelligence workloads. As organizations increasingly use external infrastructure for model training and inference, confidential execution environments can provide additional safeguards for proprietary models, user prompts and sensitive datasets.

Research is also focusing on stronger attestation mechanisms, improved hardware-software integration and protection against

microarchitectural attacks. Continuous verification of execution environments is emerging as an important direction because a platform that is trusted during initialization may still encounter security changes during runtime.

The integration of confidential computing with technologies such as secure multi-party computation, homomorphic encryption and federated learning may provide additional privacy protections for collaborative data processing. These technologies address different security requirements and can complement one another.

8. Conclusion

Confidential Computing extends conventional data protection by addressing the security of information during active processing. Through hardware-based Trusted Execution Environments, memory protection and remote attestation, it provides additional assurance that sensitive code and data are executed within an approved environment. Architectures such as Intel SGX, Intel TDX, AMD SEV-SNP and Arm CCA represent important developments in this area. Despite challenges involving side-channel attacks, performance overhead and platform interoperability, confidential computing is becoming an important component of cloud security, privacy-preserving analytics and secure artificial intelligence infrastructure.

References

[1] Confidential Computing Consortium, "Confidential Computing: Common Terminology," Linux Foundation, 2023.

[2] D. Feng, Y. Qin, W. Feng, W. Li, K. Shang and H. Ma, "Survey of Research on Confidential Computing," IET Communications, Volume 18, Issue 9, pp. 535–556, 2024.

[3] H. Birkholz, D. Thaler, M. Richardson, N. Smith and W. Pan, "Remote ATtestation procedureS (RATS) Architecture," Internet Engineering Task Force (IETF), RFC 9334, January 2023.

[4] M. Bartock, M. Souppaya, R. Savino, T. Knoll, U. Shetty, M. Cherfaoui, R. Yeluri, A. Malhotra, D. Banks, M. Jordan, D. Pendarakis, J. R. Rao, P. Romness and K. Scarfone, "Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases," NIST Interagency Report 8320, National Institute of Standards and Technology, 2022.

[5] S. Zobaed and M. Amini Salehi, "Confidential Computing Across Edge-To-Cloud for Machine Learning: A Survey Study," Software: Practice and Experience, Volume 55, Issue 5, pp. 896–924, 2025.