Proceedings of Business and Economic Studies, 2025, Volume 8, Issue 2
http://ojs.bbwpublisher.com/index.php/PBES
Online ISSN: 2209-265X
Print ISSN: 2209-2641

The Current Situation and Trends of Trusted Execution Environment Applications

Yanling Liu*, Yun Li

Hainan Vocational University of Science and Technology, Haikou 570100, Hainan, China

**Author to whom correspondence should be addressed.*

Abstract: With the rapid development of digital technologies such as big data, cloud computing, and the Internet of Things (IoT), data security and privacy protection have become the core challenges facing modern computing systems. Traditional security mechanisms are difficult to effectively deal with advanced adversarial attacks due to their reliance on a centralized trust model. In this context, the Trusted Execution Environment (TEE), as a hardware-enabled secure isolation technology, offers a potential solution to protect sensitive computations and data. This paper systematically discusses TEE's technical principle, application status, and future development trend. First, the underlying architecture of TEE and its core characteristics, including isolation, integrity, and confidentiality, are analyzed. Secondly, practical application cases of TEE in fields such as finance, the IoT, artificial intelligence, and privacy computing are studied. Finally, the future development direction of TEE is prospected.

Keywords: Trusted execution environment; Data security; Privacy protection; Cloud computing

Online publication: April 28, 2025

1. Introduction

With the rapid development of digital technologies such as big data, cloud computing, and the Internet of Things (IoT), industries and social structures around the world are undergoing profound transformation. These technological advancements have brought unprecedented connectivity, data generation, and computing power, driving innovation in areas such as smart cities, healthcare, and industrial automation. However, this technological advance has also given rise to significant challenges related to data security and privacy. Processing and storing sensitive data in a distributed environment exposes it to risks such as unauthorized access, data breaches, and cyber-attacks [1]. Traditional security mechanisms, which rely on a centralized trust model and struggle to deal effectively with advanced adversarial technologies, fall short in dealing with these threats. In this context, the concept of a Trusted Execution Environment (TEE) has emerged as a potential solution to these problems. The TEE is a secure isolated area in the processor that is used to isolate sensitive computing from the rest of the system [2]. It can ensure that the code and data within the secure zone remain confidential and tamper-proof even if the operating system or hypervisor is breached. Hardware-based TEE technologies such as Intel SGX and ARM TrustZone have received a lot of attention for their strong security capabilities in a variety of applications such as cloud computing and IoT devices [3].

The importance of TEE lies in its ability to address key security issues in modern computing environments. By isolating sensitive computing and protecting encryption keys, TEE effectively reduces the risk posed by untrusted hosts or malicious insiders. For example, in IoT applications, TEE protects the integrity of devices and prevents control logic from being tampered with by unauthorized operations [4]. In addition, TEE plays an important role in supporting the financial sector, cloud computing, and the IoT, among others. It also helps financial institutions and businesses meet increasingly stringent regulatory requirements by providing verifiable security for sensitive operations.

2. Basic concepts and technical principles of trusted execution environment

2.1. Definition of trusted execution environment

TEE is a secure area in a processor that ensures the confidentiality and integrity of code and data during execution. It operates independently of the main operating system and other applications, providing an isolated execution environment that is resistant to tampering and unauthorized access. TEE is designed to protect sensitive computing and ensure security even if the operating system or hypervisor is breached. This isolation feature makes TEE a core technology in modern secure computing systems.

2.2. The role of trusted execution environments

The primary role of TEE is to provide a trusted execution environment for critical operations, such as encrypted computing, secure data storage, and privacy protection algorithms. By isolating sensitive processes, the TEE can defend against security risks such as malware, side channel attacks, and insider threats. TEE is widely used in fields such as mobile payments, digital rights management (DRM), cloud computing, and IoT security.

2.3. Core features of a trusted execution environment

TEE's functionality is defined by the following three core features:

(1) Isolation: The TEE establishes a clear boundary between the secure environment and the rest of the system, ensuring that sensitive operations are not interfered with by untrusted components such as the operating system or other applications.

(2) Integrity: The TEE guarantees that the code executed within its premises will not be tampered with and the data processing will not be subject to unauthorized modifications.

(3) Confidentiality: The TEE protects the security of sensitive information during the calculation process and prevents the data from being accessed or leaked. This includes encryption keys, user credentials as well as the protection of proprietary algorithms.

2.4. Technical principles

TEE achieves its security objectives through the combination of hardware and software components, and its working mechanism includes the following aspects:

2.4.1. Hardware support

(1) Intel SGX (Software Protection Extension): Intel SGX creates isolated "enclaves" within the CPU's address space for the safe execution of applications. These safe zones are protected by memory encryption and prevent access by other processes and even privileged software such as the operating system [5].

(2) ARM TrustZone: TrustZone divides the processor into two worlds, which are the "Secure World" and the "Normal World." Hardware-enforced isolation ensures that sensitive computing in the secure world is not interfered with by the normal world [6].

(3) AMD SEV (Secure Cryptographic Virtualization): AMD SEV ensures data security by encrypting virtual machine memory to achieve isolation between virtual machines and between virtual machines and hypervisors.

2.4.2. Software support

(1) Remote attestation: TEE integrates basic primitives for trusted computing, such as remote authentication. Remote authentication allows an external entity to verify the integrity of the TEE environment by generating cryptographic proofs to prove its state.

(2) Security API: The TEE provides a secure application programming interface (API) that enables applications to call the TEE for encryption operations, data encapsulation, as well as secure communication.

2.5. Key components of a trusted execution environment

The TEE's functionality relies on the following key components:

(1) Secure memory: Dedicated memory areas are encrypted and isolated to prevent unauthorized access or tampering during computation [7].

(2) Trusted computing base (TCB): The TCB includes all hardware and software components that are critical to the TEE's secure properties.

(3) Encryption technology: The data processed internally by the TEE is encrypted during static storage and transmission to ensure confidentiality. The advanced encryption technology also supports secure key management and data encapsulation.

(4) Remote authentication: The remote authentication mechanism allows remote verification of the integrity of the TEE through proof of encryption, thereby enhancing trustworthiness.

3. Application status of trusted execution environment

3.1. Financial field

The financial sector is highly sensitive to data breaches, fraud, and privacy violations, so the need for secure systems is particularly pressing. TEE plays a key role in securing payment data and ensuring the privacy of transactions, as well as preventing fraud.

(1) Payment data protection: TEE isolates payment processing operations from the main operating system, ensuring the security of sensitive data such as credit card information and authentication credentials. For example, mobile payment systems such as Google Pay and Apple Pay utilize TEE to secure user data during transactions.

(2) Transaction privacy: TEE supports secure multi-party computing (SMPC) and can process transactions without exposing sensitive information. This is particularly important in cross-border payments and anti-money laundering (AML) systems, where privacy and compliance requirements are extremely high [8].

(3) Fraud prevention: By integrating machine learning models in TEE, financial institutions can detect fraudulent activity in real time while avoiding exposing sensitive data.

3.2. Cloud computing

Cloud computing has revolutionized the way data is stored and processed, but it also brings data security and privacy challenges. TEE addresses these issues effectively by enabling secure and private computing in a cloud environment.

(1) Data encryption computing: TEE allows encrypted data to be processed securely without being decrypted, thereby maintaining the confidentiality of the data throughout the calculation process. For example, the Federated Learning framework leverages TEE to train machine learning models on distributed datasets while protecting data privacy [9].

(2) Privacy protection: TEE supports a remote authentication mechanism to ensure the integrity of cloud applications. By isolating sensitive operations within a secure zone such as Intel SGX or AMD SEV, TEE provides strong security against insider threats and malicious attacks [10].

3.3. Internet of Things (IoT)

The rapid adoption of IoT devices has raised concerns about data security and privacy due to their limited computing resources and vulnerability to cyber threats. TEE offers a powerful solution for securing the IoT ecosystem.

(1) Smart device security: TEE protects critical operations on IoT devices by isolating sensitive computing from untrusted components. For example, ARM TrustZone is widely used in IoT devices to create a secure execution environment for critical operations [11].

(2) Protect against malicious attacks: By integrating blockchain technology with TEE, IoT systems can achieve decentralized access control and auditability. Smart contracts are used to enforce access rules, while the TEE ensures that sensitive data remains confidential during execution [12].

3.4. Blockchain

Blockchain technology offers decentralized security but lacks built-in privacy protections due to its transparency. TEE compensates for this shortfall by supporting confidential computing and secure smart contract execution.

(1) Privacy protection: TEE encrypts all data outside the security zone to make it unidentifiable to untrusted network nodes. This ensures that sensitive blockchain transactions are still able to maintain privacy while maintaining the integrity of the ledger [13].

(2) Secure smart contracts: By executing smart contracts in TEE, platforms like Hyperledger Fabric Private Chaincode enhance the security of decentralized applications (dApps). This approach prevents rollback attacks and ensures immutable execution [14].

3.5. Medical field

While protecting patient privacy, the healthcare industry also needs to enable secure data sharing to improve the quality of care. TEE offers a solid solution to address these challenges.

(1) Patient privacy protection: TEE isolates sensitive calculations involving electronic health records (EHRs) from untrusted environments. This prevents unauthorized access to patient information during processing or storage [15].

(2) Secure data sharing: By combining blockchain with TEE technology, healthcare systems can enable controlled sharing of patient data through smart contracts while remaining transparent and auditable. Decentralized authentication mechanisms, for example, leverage blockchain to enhance the credibility of TEE-based healthcare solutions.

4. Future trends in trusted execution environments

4.1. Next-generation TEE technology

TEE development is moving towards more efficient hardware support and flexible isolation mechanisms. Emerging hardware architectures are expected to integrate more advanced features, such as enhanced memory encryption and multi-world isolation, to address increasingly complex application needs. For example, solutions such as ARM TrustZone-M and Intel SGX are being continually optimized to reduce latency and improve scalability for resource-constrained devices such as IoT systems.

4.2. Integration with emerging technologies

TEE is deeply integrated with other advanced technologies to unlock more possibilities:

(1) Artificial intelligence (AI): TEE is critical in privacy-protected AI applications, such as Federated Learning. With TEE, data can be processed securely without exposing sensitive data. For example, TEE enables secure model training on distributed datasets while maintaining the confidentiality of the data.

(2) Blockchain: The combination of TEE and blockchain technology enhances the security of decentralized systems. TEE addresses key vulnerabilities in distributed ledger technology by providing a trusted environment for executing smart contracts and ensuring the privacy of blockchain transactions.

4.3. Privacy computing

TEE becomes indispensable in privacy computing applications:

(1) Federated learning: TEE supports secure aggregation of distributed data in the Federated learning framework. This approach is widely used in healthcare and smart city solutions to train AI models without compromising user privacy.

(2) Data sharing: In scenarios that involve sensitive data sharing, such as cross-agency collaboration, TEE ensures that data is protected at all times during processing. This is particularly important in industries such as finance and healthcare.

4.4. 5G and edge computing

The deployment of 5G networks and the rise of edge computing bring new opportunities for TEE applications:

(1) Low-latency processing: TEE is ideal for edge devices that require low-latency secure processing. By performing secure computations close to the data source, TEE reduces the need to transfer data to a centralized server.

(2) Smart infrastructure: In a 5G-enabled environment, TEE enhances the security of critical infrastructure by protecting critical operations from cyber threats.

5. Conclusion

This paper analyzes the technical principles of TEE and its wide application in the fields of finance, IoT, artificial intelligence, and privacy computing, demonstrating its key role in scenarios such as payment data protection, privacy-protected federation learning, and blockchain smart contract execution. At the same time, the paper also explores the future development trend of TEE. In the future, with the improvement of hardware efficiency and the improvement of the ecosystem, TEE will further promote innovative development in areas such as privacy computing, distributed systems, and edge computing, laying the foundation for building a more secure and trusted digital society.

Disclosure statement

The authors declare no conflict of interest.

References

[1] Stergiou C, Bompoli E, Psannis K, 2023, Security and Privacy Issues in IoT-Based Big Data Cloud Systems in a Digital Twin Scenario. Applied Sciences, 13(2): 758. https://doi.org/10.3390/app13020758

[2] Witharana H, Weerasena H, Mishra P, 2024, Formal Verification of Virtualization-Based Trusted Execution Environments. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 43: 4262–4273.

[3] Liu Z, Hu C, Li R, et al., 2023, A Privacy-Preserving Outsourcing Computing Scheme Based on Secure Trusted Environment. IEEE Transactions on Cloud Computing, 11: 2325–2336.

[4] Valadares D, Sobrinho D, Perkusich A, et al., 2021, Formal Verification of a Trusted Execution Environment-Based Architecture for IoT Applications. IEEE Internet of Things Journal, 8(23): 17199–17210.

[5] Kuniyasu S, 2020 Implementation of Trusted Execution Environment and Its Supporting Technologies, IEICE ESS Fundamentals Review, 14(2): 107–117.

[6] Xia J, Pan D, Pan Y, et al., 2022, User-level Enclave Protection Scheme based on ARM TrustZone. In International Conference on Frontiers of Electronics, Information and Computation Technologies (ICFEICT 2021). Association for Computing Machinery, New York, NY, USA, 138: 1–6. https://doi.org/10.1145/3474198.3478243

[7] Witharana H, Chatterjee D, Mishra P, 2024, Verifying Memory Confidentiality and Integrity of Intel TDX Trusted Execution Environments. *2024 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 44–54.

[8] Yi H, 2024, Anti-Money Laundering (AML) Information Technology Strategies in Cross-Border Payment Systems. *Law and Economy*, 12(1): 55–70.

[9] Li Z, He S, Chaturvedi P, et al., 2024, Secure Federated Learning Across Heterogeneous Cloud and High-Performance Computing Resources — A Case Study on Federated Fine-tuning of LLaMA 2. *Computing in Science & Engineering*, 26(2): 120–130.

[10] Reddy K, Chadha A, Nikhil P, et al., 2024, Hybrid Cryptography Techniques for Data Security in Cloud Computing. *2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT)*, 5: 1836–1842.

[11] Segarra C, Delgado G, Schiavoni V, 2020, MQT-TZ: Hardening IoT brokers using ARM TrustZone: (Practical experience report). *2020 International Symposium on Reliable Distributed Systems (SRDS)*, 256–265.

[12] Jiang W, Li E, Zhou W, et al., 2023, IoT Access Control Model Based on Blockchain and Trusted Execution Environment. *Processes*, 11(4): 813–822.

[13] Lew C, Torres C, Shinde S, et al., 2024, Revisiting Rollbacks on Smart Contracts in TEE-protected Private Blockchains. *2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 217–224.

[14] He J, Cao D, Zhou Y, 2022, TrustAuction: A TEE based Privacy Protection Framework for Auction Contracts. *2022 IEEE 22nd International Conference on Software Quality, Reliability, and Security Companion (QRS-C)*, 766–767.

[15] D'Antonio, S, Giglio J, Mazzeo G, et al., 2024, Enhancing Healthcare Data Confidentiality through Decentralized TEE Attestation. *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, 676–681.