International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

RELIABLE EXECUTION ENVIRONMENTS FOR INTERNET OF THINGS APPLICATIONS USING CLOUD/FOG

S. Kesavan[1] and S. Srinivasan*[2]

[1] Department of Computer Science and Engineering, AMET University, Chennai, India

[2] Professor, Department of Advanced Computing Sciences, AMET University, Chennai, India.

Abstract:

The Internet of Things (IoT) can communicate and process information more efficiently with the use of cloud services and fog-based solutions. IoT solutions can do more complex tasks in shorter amounts of time because to cloud and fog servers' increased processing capability, which is not achievable when depending only on IoT devices. Since IoT devices can barely handle complicated security responsibilities, the advantages of cloud and fog computing are much greater when sensitive data processing is taken into account. Trusted Execution Environments (TEEs) enable the processing of sensitive data and code within secure, separated memory regions, hence enhancing data security in cloud/fog-based IoT applications. This article presents a brief overview of the usage of TEEs to protect data in cloud/fog-based Internet of Things applications. We highlight key research problems and directions while concentrating on solutions based on the two top TEE technologies currently on the market (Intel SGX and ARM Trust zone).

Keywords: Internet of Things, ARM Trust Zone, Intel SGX, fog computing, security, and trusted execution environments.

INTRODUCTION:

When paired with the cloud or fog computing paradigm, the Internet of Things (IoT) paradigm has become more powerful. By enabling applications requiring complicated and quick processing to run in fog/cloud servers, this combination allays worries about the normal limitations of IoT devices, such as limited memory and processing capabilities. Notwithstanding these advantages of fog and cloud computing, issues still arise when sensitive data is handled by cloud/fog-based Internet of Thing applications.

Trusted Execution Environments (TEEs) are one of the frequently used methods to protect data produced by Internet of Things applications. One definition of TEE is a tamper-resistant processing environment provides the run code with a sufficient degree of confidentiality, integrity, and authenticity (Sabt et al., 2015). A TEE should provide a remote attestation procedure so that other parties can verify its reliability. However, an opponent can still use Side-Channel assaults, hence TEE is not a foolproof solution for systems security[1]. Through its TEE System Architecture and API specifications, which include the TEE Client API, TEE Internal Core API, and TEE Secure Element API, among others[3], Global Platform [2] has been in charge of TEE standardization since 2010.

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

To investigate how TEE intends to protect data in cloud/fog-based IoT applications, we developed the following research questions:

1. What suggestions are there right now for using TEE in IoT applications?
2. What kinds of IoT solutions does TEE currently employ?

We conducted a basic literature research in order to find relevant publications in some of the major scientific archives for computer science (e.g., Scopus4, IEEE Digital Library5, and ACM Digital Library6). The following keywords were used as search topics for this search: "Internet of Things," "Trusted Execution Environment," and "Security." Only the two primary TEE technologies on the market—Intel SGX and ARM TrustZone—have been considered. Ten publications were chosen for each TEE technology, which is adequate to give an overview of the research completed so far and to offer recommendations for further investigation. The following is a list of our primary contributions:

- A TEE survey that presented pertinent linked papers and was used to safeguard cloud/fog-based IoT applications;
- A conversation about the main study areas and the difficulties in using TEE for IoT applications;
- A place to start when conducting a Systematic Literature Review in relation to the research questions.

As far as we are aware, this paper is the first review of TEE's utilization in IoT applications. This paper's remaining sections are organized as follows. The basics of ARM Trust Zone and Intel SGX are covered in Section 2, while works that incorporate Intel SGX in their proposals are presented in Section 3. Finally, works pertaining to the context of ARM Trust Zone are covered in Section 4. The primary weaknesses of the two TEE technologies under discussion are shown in Section 5. We outline pertinent obstacles and future directions for TEE's use in the Internet of Things in Section 6, and in Section 7, we go over related literature. Section 8 then lays out the conclusions.

2 BACKGROUND

The two most popular TEE technologies on the market right now—Intel Software Guard Extensions and the ARM Trust Zone—as well as some of their distinctions and typical IoT application scenarios are briefly described in this section.

2.1 Extensions for Intel Software Guard (SGX)

Applications can operate in a secured memory space known as an enclave that houses the application code and data thanks to Intel Software Guard Extensions (Intel SGX), an extension to the x86 architecture instruction set. According to McKeen et al. (2013), Jain et al. (2016), and da Rocha et al. (2020), an enclave is a protected area in the application's address space that ensures the confidentiality and integrity of the data, preventing malware and even other software with high execution privileges, like VM monitors, BIOS, and the operating system, from accessing this data. As illustrated in Fig. 1, we describe the attack surface of an SGX enclave.

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

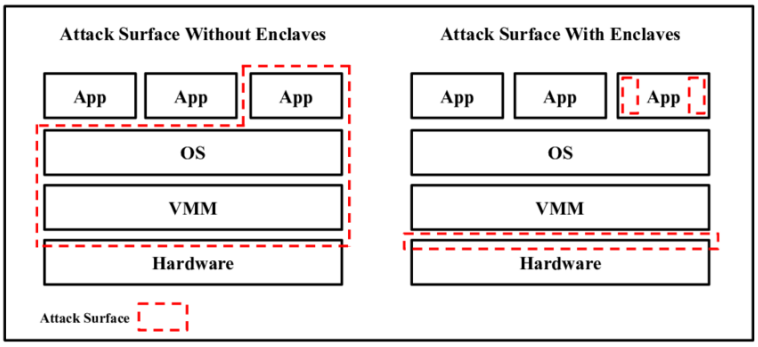


Figure 1: Attack surface of a security-sensitive application without SGX enclaves (left) and with SGX enclaves (right).

Memory encryption uses standard techniques that offer defences against replay attacks. Every time the system restarts or hibernates, the encryption key is randomly changed and kept in registers inside the CPU that are inaccessible to external components (Intel, 2016b). Every enclave has a document bearing the signature of the author of the enclave and contains details that enable the Intel SGX architecture to determine whether any enclave components have been altered. But only after the enclave is loaded does the hardware verify its dimensions (Intel, 2016a).

When applications wish to store their keys and data outside of the enclave's security, like on disk, they can additionally ask the enclave for a special key, known as a sealing key, to safeguard them. Additionally, enclaves can attest to one another, allowing for the establishment of a secure communication channel for the exchange of sensitive data (Anati et al., 2013).

SGX's primary objective is to decrease the Trusted Computing Base (TCB) so that only sensitive application components can be housed in enclaves. There are certain benefits to dividing a program into two parts. The trusted portion of the application has fewer points of failure, making the software safer.

2.2 ARM TrustZone

ARM Any component of the system can be safeguarded thanks to the hardware architecture known as Trust Zone, which addresses the security element of the system design as a whole. Trust-Zone technology offers a foundational framework that enables SoC designers to select a variety of components capable of supporting particular tasks in a safe setting. The primary objective of the architecture is to make it possible to create a programmable environment that can be used to create a set of security solutions that are not achievable with conventional techniques and safeguard the confidentiality and integrity of nearly all assets against particular attacks. (ARM, 2009).

A secure world and a regular world are the two logical states in which the system can be isolated using the ARM Trust Zone architecture (Fig. 2). Through the system bus, these states are also communicated to all peripheral devices, enabling them to base their judgments about access control on the state of the system. Monitor is the mechanism in charge of exchanging context between the two states.

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

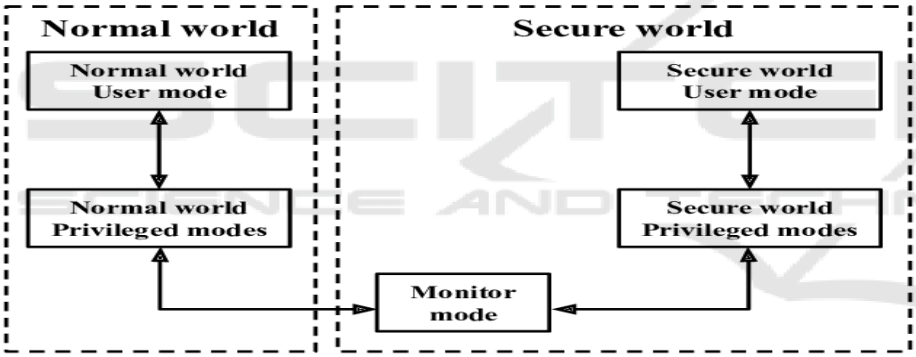


Figure 2 **:** Execution modes in the ARM TrustZone archi- tecture.

Applications operating in a secure environment are able to isolate certain memory areas for their usage, restricting access from applications operating in a regular environment. Such isolation is ensured by the memory controller that uses the Trust Zone architecture premises, which provide access control for memory regions according to the current state. Runtime programming or static memory partitioning are also possible.

Applications that operate in a secure environment can also make certain exceptions or interrupts only be caught in a secure environment; this control is also in charge of the interrupt controller. In order to guarantee that these devices are only used by secure applications, the system can additionally prevent access to certain devices for apps that are not operating in a secure environment (Lesjak et al., 2015).

2.3 Distinctions between Intel SGX and ARM Trust Zone

The key features of the Intel SGX TEE and ARM Trust-Zone technologies are contrasted in Table 1. It is evident that Intel SGX technology encompasses the essential features required to create secure apps without relying on the operating system or other highly privileged components. Additionally, ARM Trust Zone can offer compatible devices a reliable communication channel.

Table 1: Comparison between the ARM Trust Zone and Intel SGX TEE technologies

	ARM TrustZone	Intel SGX
Architecture	ARM	x86-64
Secure Storage		C
Attestation		C
Memory Isolation	C	C
Cryptographic Accelerator	C	C
Trusted I/O	C	

While Intel SGX technology seeks to provide a comprehensive solution for the connection between CPU and memory components, ARM Trust Zone is devoid of a component that can

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

provide a trusted code measurement. The safe storage and attestation techniques are based on a device-unique key. Such characteristics can be provided in conjunction with a TPM or another module that can provide a unique key and code measurement.

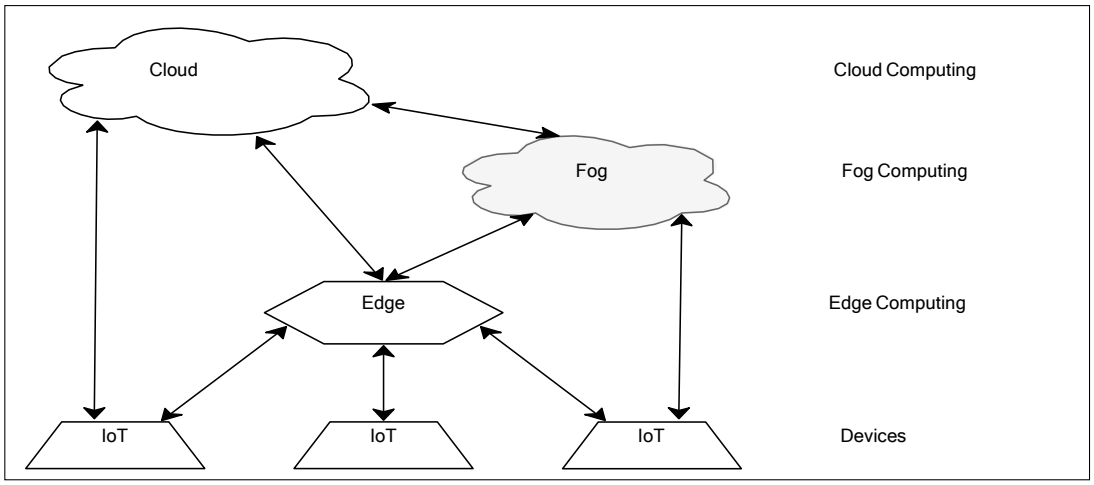
In contrast to ARM Trust Zone, Intel SGX technology focuses solely on CPU and memory connectivity and does not have a native functionality to enable secure communication with I/O devices. To provide the previously specified secure connection, Intel SGX must be used in conjunction with other solutions, such as trusted path designs based on hypervisors (Weiser and Werner, 2017).

2.4 Typical IoT Situations

IoT applications are typically distributed systems that involve a variety of servers, platforms, and devices. As previously stated, the various IoT scenarios require cloud, fog, and edge computing paradigms to address the limitations of the known devices. In Fig. 3, we display the typical IoT scenarios taking these paradigms into account.

The IoT devices that gather environmental data are the primary entities. The devices have the option of processing this data locally or sending it to a cloud server, fog server, or edge gateway. If additional processing, memory, and storage are required, an edge gateway can additionally connect to a fog or cloud server. Data interaction between the cloud servers and fog servers is also possible. The communication options are shown by the arrows in Figure 3. Between the gadgets and the layers of fog, clouds, and the edge

Figure 3: Common Scenarios for IoT Applications.



Given these typical situations, we can consider using TEE in any combination to safeguard sensitive data. Since the Trust Zone's architecture can be found in a wide range of ARM processor-based devices, including micro-controllers, it is better suited for the Internet of Things. In contrast to Trust Zone, SGX is limited to machines with Intel processors. In this manner, TEE is frequently applied to edge gateways or fog/cloud servers in systems that use trusted apps to protect data in various IoT contexts.

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Intel SGX and ARM Trust Zone technology can be combined in IoT solutions. Fog and cloud servers are utilized for the second one, while IoT and edge devices are employed for the first to ensure trustworthy operations. After leaving the devices, data is protected in transit using cryptography techniques and secure protocols (such as Transport Layer Security). Devices can operate in a closer edge gateway if they lack the capacity to handle such security responsibilities. In order to enable a fog/cloud server to verify IoT/edge devices and establish a reliable communication channel between them, Intel SGX offers methods to carry out a remote attestation procedure with third parties.

3 . SGX INTEL SOLUTIONS

A blockchain that employs a proof of lucky consensus protocol was introduced by Milutinovic et al. (Milutinovic et al., 2016). A random number generator based on a Trusted Execution Environment achieves minimal transaction validation latency, low energy usage, and deterministic confirmation time. The authors described the protection offered by this method and used Intel SGX capabilities for this.

To achieve accountability for data access and safeguard sensitive health data, Liang et al. (Liang et al., 2017) suggested utilizing blockchain technology and Intel SGX. Patients can gather and manage their health data with the help of a proposed user-centric personal health data management system. The authors claim that the plan accomplishes self-sovereign data ownership, scalable processing, decentralized and distributed privacy, access control, permanent data records with integrity, and trustworthy responsibility.

A data dissemination platform with data security and privacy levels was proposed by Sampaio et al. (Sampaio et al., 2017). The suggested system allows data producers complete control over consumer access, allowing them to choose the granularity level and grant or refuse consumers access to sensitive data. By leveraging Intel SGX, trusted entities can create sensitive data, anonymize it repeatedly, or aggregate it before allowing untrusted programs to use it, protecting the privacy of the original data. Compared to homomorphic encryption, the technique is more practical due to the utilization of Intel SGX. The solution, which had a lower overhead and could be helpful for medium-sized systems with modest data dissemination volumes, was assessed by the authors.

Because exchanging location traces with untrusted service providers may have privacy issues, SGX is also used to protect user privacy in location-based services. In order to create a secure channel between the device and the enclave and enable the exchange of sensitive information, Kulkarni et al. (Kulkarni et al., 2017) described an architecture in which the user device (IoT, mobile phone, or GPS-enabled device) starts an attestation process with an enclave that operates in an untrusted provider. To prevent data from leaking to an untrusted cloud, all user data is processed inside an enclave. Spatial-cloaking with k-anonymity is a superior solution than what is currently available, according to the authors, who examined the solution with a negligible overhead and near-perfect outcomes.

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Log Safe, a distributed, scalable, fault-tolerant, and reliable logger for data from IoT devices, was proposed by Nguyen et al. (Nguyen et al., 2018). The suggested logger uses Intel SGX to offer tamper detection, protect against replay, injection, and eavesdropping threats, and satisfy confidentiality, integrity, and availability requirements. Log Safe's excellent scalability, as shown by experiments, enables it to function with a large number of IoT devices and a high data transfer rate.

Table 2: Summary of Intel SGX solutions.

Title	Year	Solution
Proof of Luck: an Efficient Blockchain Consensus Protocol (Milutinovic et al., 2016)	2016	Blockchain Consensus Protocol
Towards Decentralized Accountability and Self-Sovereignty in Healthcare Systems (Liang et al., 2017)	2017	Personal Health Data Management system
Secure and Privacy-Aware Data Dissemination for Cloud-based Applications (Sampaio et al., 2017)	2017	Data Aggregation and Dissemination Platform
Privacy-Preserving Location-Based Services by Using Intel SGX (Kulkarni et al., 2017)	2017	Secure Architecture for Location-based Services
LogSafe: Secure and Scalable Data Logger for IoT Devices (Nguyen et al., 2018)	2018	Trusted logger
Decentralized IoT Data Management Using BlockChain and Trusted Execution Environment (Ayoade et al., 2018)	2018	Descentralized Data Management system
BASTION-SGX: Bluetooth and Architectural Support for Trusted I/O on SGX (Peters et al., 2018)	2018	Bluetooth Trusted I/O
Security and privacy aware data aggregation on cloud computing (Silva et al., 2018)	2018	Smart Metering Data Aggregation
Achieving Data Dissemination with Security using FIWARE and Intel Software Guard Extensions (Valadares et al., 2018)	2018	Trusted Architecture
Enabling Security-Enhanced Attestation With Intel SGX for Remote Terminal and IoT (Wang et al., 2018)	2018	Security-enhanced Attestation

Using blockchain and TEE technologies, Ayoade et al. (Ayoade et al., 2018) suggested a decentralized approach for data management in Internet of Things applications. Using blockchain smart contracts and storing just data hashes in the blockchain—while retaining raw data in a TEE application—the objective is to establish access control. The Ethereum blockchain and Intel SGX were used by the authors to develop the idea, and they conducted experiments on the processing costs at the blockchain and SGX application (gas usage,

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

throughput, and CPU time considering the primary operations). The results show that the efficiency of the solution is satisfactory.

BASTION-SGX, an architectural support for Bluetooth trustworthy I/O utilizing Intel SGX, was proposed by Peters et al. (Peters et al., 2018). The objective of this work is to safeguard I/O data even when high-level privilege advertisements are taken into account. The authors discussed the difficulties in designing and implementing "trusted I/O," offered a potential fix, and detailed the deployment of a proof-of-concept that secures data between the SGX enclave and the Bluetooth controller by extending the current Bluetooth security. A secure tunnel connecting the Bluetooth hardware and an SGX enclave is part of the solution.

An architecture for data aggregation in cloud computing was given by Silva et al. (Silva et al., 2018), taking into consideration two methods for data security and privacy. The message bus, producers, aggregators, and consumers are the four primary parts of the suggested architecture. In order to assess the reaction time to conduct common tasks in smart metering, such as instant energy consumption and monthly bill computations, proofs of concept were put into practice. One aggregator that took into account the Intel SGX technology and another that took into account a homomorphic encryption approach were both put into practice. Tests were conducted with the host computer, virtual machines, and containers in mind. The obtained outcomes show that, in comparison to the homomorphic encryption method, Intel SGX allows for faster reaction times. The authors also provided a security study and listed the benefits and drawbacks of each strategy.

Valadares et al. suggested a trusted architecture that uses Intel SGX to safeguard private information in Internet of Things applications (Valadares et al., 2018). The proposal incorporates cryptography, trusted processing using a TEE, authorization, and authentication into a standard publish/subscribe architecture. The authors tested the proposal's time overhead by implementing a prototype and comparing it to a solution without any security measures. The findings showed a high degree of scalability and little overhead for all communication flows with the security procedures.

Wang et al. (Wang et al., 2018) suggested a security-enhanced attestation for IoT devices and remote terminals that is appropriate for use with enterprise networks' "bring your own device" policy. With a limited trusted computing base and dynamic attestation based on several enclaves, the approach offers protected execution for measurements and attestation. It also offers a policy-based measurement mechanism that, thanks to SGX, allows administrators to gather and keep an eye on the run-time status in a reliable manner. There is some overhead in the testing process for the assessed prototype.

Table 2 lists all ten of the publications that employed Intel SGX to offer data security solutions for fog/cloud-based Internet of Things applications.

4. SOLUTIONS FOR ARM TRUST ZONES

An architecture for a trusted embedded operating system that complies with Global Platform TEE requirements was introduced by Yang et al. (Yang et al., 2014). The authors created and

Received: August 03, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

executed the Trust-E solution, and as a demonstration, they constructed a mobile payment application to assess the efficacy and accuracy of their system. The authors claim that the findings showed how well the suggested method could satisfy the security specifications.

Lesjak et al. (Lesjak et al., 2015) designed and implemented a device snapshot authentication system as part of their security solution proposal for industrial maintenance scenarios. By comparing the two technologies, this approach was put into practice using ARM Trust Zone and Security Controller. According to the findings, the Security Controller solution offers superior defence against physical threats, while the Trust Zone solution offers more performance and flexibility. The writers came to the conclusion that the use case determines the technology that is selected. They suggested a hybrid approach that makes use of both technologies to optimize security and performance: using Security Controller in software components that require more security and Trust Zone in software components that require more processing power.

Table 3: Summary of ARM Trust zone solutions

Title	Year	Solution
Trust-E: A Trusted Embedded Operating System Based on the ARM Trustzone (Yang et al., 2014)	2014	Trusted Embedded Operating System Architecture
Hardware-security technologies for industrial IoT: TrustZone and security controller (Lesjak et al., 2015)	2015	Device Snapshot Authentication System
CacheKit: Evading Memory Introspection Using Cache Incoherence (Zhang et al., 2016)	2016	Processor Cache Exploitation through a Rootkit
OPTZ: a Hardware Isolation Architecture of Multi-Tasks Based on TrustZone Support (Dai and Chen, 2017)	2017	Multitask Hardware Isolation Architecture
TM-Coin: Trustworthy Management of TCB Mveasurements in IoT (Park and Kwangjo Kim, 2017)	2017	Trustworthy TCB Measurements Management System
LTZVisor: TrustZone is the Key (Pinto et al., 2017)	2017	Hypervisor to Assist Virtualization
Secure Edge Computing with ARM TrustZone (Pettersen. et al., 2017)	2017	Trusted Edge Computing Platform
A TrustEnclave-Based Architecture for Ensuring Runtime Security in Embedded Terminals (Chang et al., 2017)	2017	Runtime Security for Embedded Terminals
TruApp: A TrustZone-based authenticity detection service for mobile apps (Demesie Yalew et al., 2017)	2017	Mobile App Authenticity and Integrity Checker
Building a Trustworthy Execution Environment to Defeat Exploits from both Cyber Space and	2019	Shield System for Legacy Applications

Received: August 03, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Physical Space for ARM (Guan et al., 2019)		

In order to demonstrate the viability of introducing malicious code into the processor cache while concealing it, Zhang et al. (Zhang et al., 2016) provided a systematic investigation of cache incoherence behavior between regular and secure worlds in the ARM Trust-Zone. They also suggested a rootkit named Cachekit. The incoherent state between the secure and regular worlds made it feasible for the rootkit to avoid detection tools' introspection. In terms of detection techniques, the authors contrasted the Cache kit with other rootkits. Since the malicious code entirely hides inside the cache, it turned out to be the best method without being detected.

The design and implementation of OPTZ (Open Trust-Zone), a multitask hardware isolation between regular and secure worlds, was proposed by Dai and Chen (Dai and Chen, 2017). Its architecture consists of a secure operating system (for the secure world), a standard operating system (for the ordinary world), secure services, and a communication mechanism. Taking into account a multitask hardware isolation and a system interrupt architecture, the authors concentrated on the communication between the regular and secure worlds via the secure monitor. Using the Trust Zone technology, they put the architecture into practice and tested the physical memory access in order to confirm its accuracy. The results demonstrated the effectiveness of the proposed hardware isolation.

A reliable management solution for TCB (Trusted Computing Base) measurements from Internet of Things applications was proposed by Park and Kim (Park and Kwangjo Kim, 2017). The system, which employs blockchain and Trust Zone, was dubbed TM-Coin by the authors. In order to safely distribute the TCB measurements throughout the blockchain, they pre-sent the protocol and transaction flow. The TM-Coin transactions that contained the TCB measurements were generated and secured using TrustZone. Through tests using a working prototype, the solution created a remote attestation mechanism and assessed its performance overhead.

LTZVi-sor, a hypervisor that leverages TrustZone to support virtualization, was proposed by Pinto et al. (Pinto et al., 2017). The hypervisor architecture and implementation details were supplied by the authors. Three metrics were taken into consideration throughout the experimental evaluation: memory footprint, performance overhead, and interrupt latency. When running unaltered rich operating systems, the testing findings showed a low-performance overhead, meeting the stringent requirements for real-time environment virtualization.

ARM TrustZone and Intel SGX were both utilized by Pettersen et al. (Pettersen et al., 2017) to develop a generic platform that allows cloud, mobile, and IoT devices from many vendors to integrate and interact seamlessly in a secure and privacy-preserving way. Three layers are piled vertically in the suggested construction. The client device at the topmost layer is ARM TrustZone enabled. In the same administrative domain, the middle layer is also a client device, like an enterprise cloud server or fog de- vice, that has ARM TrustZone or Intel SGX

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

capabilities. The public cloud, which has Intel SGX enabled, makes up the third layer. With minimal overhead, the solution integrates IoT edge devices to back-end cloud servers in a safe manner.

Chang et al. (Chang et al., 2017) suggested using TEE to effectively handle runtime security issues since it makes use of hardware isolation technology. They described the basic operation of the TrustZone architecture, which is separated into regular and secure worlds (untrusted and trusted, respectively). In order to assess the proposal, they tested a Trust Zone-enabled hardware device, which produced experimental findings proving its viability and efficacy.

Yalew et al. (Demesie Yalew et al., 2017) introduced TruApp, a tool that verifies a mobile application's integrity and authenticity by examining certain measurements, static and dynamic watermarks, and a verification key provided by the TruApp provider or app manufacturer. TruApp is secure because it checks the portion running in the insecure world while executing mostly in a TrustZone secure environment. Following trials and implementation of the concept, the authors came to the conclusion that while the metrics are more successful in identifying fraudulent apps, they come with higher overhead expenses. They suggested that future research examine ways to optimize the TruApp.

A new approach called Trust-Shadow was proposed by Guan et al. (Guan et al., 2019) to protect legacy apps on multiprogramming IoT devices from untrusted operating systems. It makes use of ARM TrustZone technology, which protects vital applications by using a lightweight run-time framework that handles communication between the OS and the applications in the real world. This runtime system does not provide system services. To safeguard all the data segments from a security-critical application, it uses a page-based encryption technique that forwards queries from the untrusted ordinary world while confirming the answers. The internal RAM decrypts the encrypted page whenever it is visited, making it impervious to physical attacks. Modifications to legacy apps are not required. Microbenchmarks and real applications were used to test the suggested method, and the results showed minimal and occasionally moderate overhead when using real applications.

Table 3 contains a list of all ten of these published papers along with their solutions that took into account using ARM Trustzone to enhance or offer data security in Internet of Things applications.

5. TRUSTZONE AND SGX VULNERABILITY

The threat models of Intel SGX and TrustZone do not take side-channel or reverse-engineering threats into account. According to the Intel Software Guard Extensions Development Guide (Intel, 2016a), developers are responsible for creating enclaves that are impervious to these kinds of attacks. Side-channel attacks may produce sufficient information to allow the attacker to deduce the order in which instructions are being executed, or passive address translation attacks may provide the attacker with information about memory access patterns at the page level. Wang et al. (2017) categorize these vulnerabilities into four attack vectors: branch timing, cache miss statistics, power statistics, and page accesses through page tables.

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

AI: The data in cache memory in SGX apps is in plain-text, even though the enclave is cryptographically secured in the EPC. Even though the untrusted world (ordinary world) cannot access the secure cache lines, the same thing happens for Trust-Zone programs (Lesjak et al., 2015; Cerdeira et al., 2020).

Sensitive information, including AES keys (Moghimi et al., 2017) and RSA processing keys (Schwarz et al., 2017; Brasser et al., 2017), could be extracted from enclaves via side-channel in a number of works in the literature. Additionally, secrets within an SGX enclave (Chen et al., 2019a) or TrustZone trusted applications (Guan et al., 2019) can be deduced using spectre vulnerabilities. Shih et al. (Shih et al., 2017) suggest T-SGX in an effort to lessen the impact of side-channel attacks in applications that employ SGX. In order to eliminate the impact of known side-channel attack approaches, Transactional Synchronization Extensions (TSX) resources are used to isolate attempts at unauthorized access to the enclave data.

Using strategies like use-after-free and time-of-check-to-time-of-use, Weichbrodt et al. (Weichbrodt et al., 2016) also tackle thread synchronization problems in enclaves. By doing so, the attacker can circumvent enclave access controls or take over the flow of control, interrupting threads and causing segmentation failures in enclaves.

6. DIFFICULTIES AND ADVICE

When creating reliable and effective solutions, one must consider the difficulties presented by the use of TEE. Nonetheless, effective measures to guarantee the security of an application's data are provided by the Intel SGX architecture. The architecture's threat model excludes side-channel and reverse-engineering assaults. Applications outside of the enclave can thereby affect an enclave's code execution prediction, making the SGX architecture susceptible to Spectre attacks. An adversary can learn secrets from the enclave's memory or registers by manipulating the control flow to carry out instructions that result in observable cache state changes (Chen et al., 2019b).

Techniques like use-after-free and time-of-check-to-time-of-use are also used to address thread synchronization issues in enclaves. These techniques interrupt threads and force segmentation failures in enclaves, enabling the attacker to take over the control flow or get around enclave access controls (Weichbrodt et al., 2016). (Beekman and Porter, 2017) explore some of the difficulties in implementing the remote attestation protocol in order to create scalable and secure apps with SGX.

As demonstrated by Lipp et al. (Lipp et al., 2016), who use the ordinary world to monitor operations carried out in the Trust-Zone secure realm, the ARM TrustZone architecture is also vulnerable to side-channel assaults. Additionally, there are a number of security warnings pertaining to TrustZone, including kernel and driver flaws as well as hardware vulnerabilities that impact various platform hardware components (Pinto and Santos, 2019).

Although software writers must take into account defects and vulnerabilities in both hardware and software components, they may believe that TEE is completely safe. Performance concerns in both ARM TrustZone and Intel SGX must also be taken into account. Ning et al. provide a wide range of perspectives on the difficulties with TEEs (Ning et al., 2017).

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

As shown in Fig. 4, we may aggregate the crucial answers from the chosen articles for both the Intel SGX and the ARM Trust-Zone in order to determine the future areas of future study. Among the suggested solutions, we observed that both of the discussed TEE technologies had been used to provide security for data aggregation and management systems. We found ideas pertaining to trusted architectures, attestation, and trusted logging and I/O operations systems when we simply looked at Intel SGX solutions. We found proposals pertaining to rootkits, trusted operating systems and hypervisors, authentication and authenticity systems, trusted platforms for edge computing, and protection for embedded terminals and legacy systems when we solely looked at ARM Trust Zone solutions.

For any IoT ecosystem, it is critical to secure the firmware update process for IoT devices. Any IoT device's firmware should be updated via a dependable and secure method that enables it to revert to a previous operational state in the event that the update fails (due to an unintentional or deliberate error). In this regard, Surdu (Surdu, 2018) offers a TEE-based technique that separates the primary players in the firmware update procedure. To prevent any interference with the current functioning system, the updated firmware is appropriately instantiated in a staged TEE zone and interfaces with emulated drivers during the upgrade process. The system switches to the new configuration after the updated firmware is completely operational; Otherwise, it keeps using the firmware that was previously functional.

As may be observed, TEE can be used to investigate a wide range of subjects and provide a number of solutions. The following features of blockchain, a related topic that was found among the solutions using both SGX and Trust Zone, are highlighted:

1. Encrypted and safely stored locally or on a secure server (such as the cloud or fog);
2. The blockchain infrastructure contains the data hashes.

To do this, TEE is a choice for performing sensitive data operations (encryption, decryption, and processing) while maintaining the security of cryptographic keys. We recommend using TEE for the most important parts of the application, which could be targeted by hostile actors without authorization.

7. CONNECTED WORK

The Internet of Things' trust and security issues have been studied, solutions have been proposed, and many technologies have been investigated for these solutions. As anticipated, surveys and reviews were conducted to map these trust and security efforts based on this promising and expansive research topic.

Aly et al. (Aly et al., 2019) concentrated on enumerating and talking about works that dealt with security threats and difficulties in general. Some surveys, like Kouicem et al. (Kouicem et al., 2018) and Di Martino et al. (Di Martino et al., 2018), parallel how each cited work relates to trust and security issues while presenting more general research and discussion about various IoT aspects, such as interoperability and architecture. The Trusted Execution Environment and its use with Edge/Fog solutions, however, are not covered in any of these surveys.

A survey of hardware-assisted security solutions with an emphasis on edge computing scenarios was presented by Coppolino et al. (Coppolino et al., 2019). Their work presents a

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

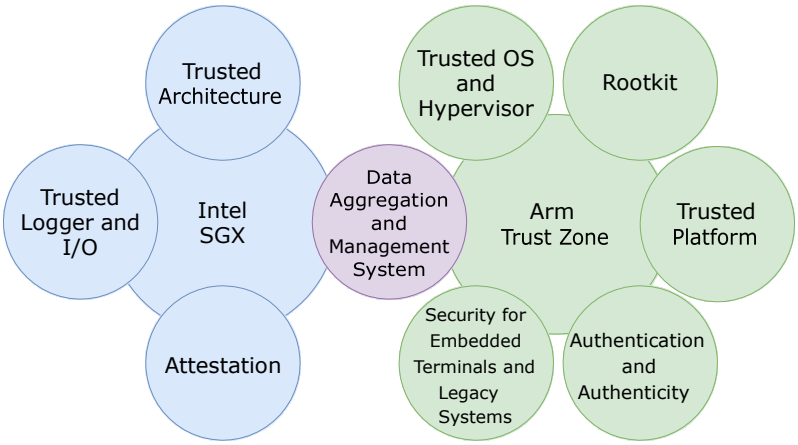
variety of hardware-assisted security technologies, including the possible application of Trusted Execution Environments. A detailed review of works that investigate TEE technology in their solutions—including their application in Edge and Internet of Things scenarios—is not provided, nevertheless.

Thus, as far as we are aware, there isn't a published survey, mapping, or assessment of the many applications of TEE for IoT applications at this time.

8. FINAL RESULTS

In order to collect pertinent articles about the application of TEE in cloud and fog-based solutions to enhance security, we conducted a literature review for this project for applications involving IoT data. We compiled the solutions and examined potential problems and future research directions. We concentrated on 20 published publications for this study: Ten solutions based on Trust Zone and ten based on SGX

Figure 4: Key solutions found in the selected papers



We discussed the primary issues surrounding the usage of TEEs and provided summaries of each chosen publication. Additionally, we continued a brief conversation about the primary research areas addressed by TEEs' use and advancements, including secure storage, authentication, virtualization, and private and sensitive data processing. We intend to conduct a systematic literature review in the future, concentrating on all pertinent studies that have been published in prestigious journals and conferences.

REFERENCES:

1. In 2019, Aly, M., Quintero, A., Haoues, M., Khomh, F., and Yacout, S. A comprehensive survey of the literature on enforcing security in internet of things frameworks. Page 100050 of Internet of Things.
2. Scarlata, V. R., Johnson, S. P., Gueron, S., and Anati, I. (2013). cutting-edge technology for CPU-based sealing and authentication. Published in Tel-Aviv, Israel, at the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy. ACM

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3. ARM (2009). Technology for security: Using TrustZone technology to create a secure system (white paper). ARM Limited.
4. Hamlen, K., Khan, L., Karande, V., and Ayoade, G. (2018). Blockchain technology and a trustworthy execution environment are used for decentralized IoT data management. IEEE International Conference on Integration and Reuse of Information.
5. Porter, D. E. and Beekman, J. G. (2017). scalability issues for apps in different enclaves. New York, NY, USA: Proceedings of the Second Workshop on System Software for Trusted Execution. ACM.
6. Kostiainen, K., Capkun, S., Sadeghi, A.-R., Brasser, F., Mu¨ller, U., and Dmitrienko, A. (2017). Software Grand Exposure: It is feasible to launch SGX cache assaults. In Proceedings of the 11th USENIX Workshop on Offensive Technologies, USENIX Association, Vancouver, British Columbia, Canada´.
7. Fonseca, P., Cerdeira, D., Santos, N., and Pinto, S. (2020). SoK: Recognizing the Most Common Security Flaws in TrustZone-Assisted TEE Systems. Proceedings of the IEEE Symposium on Privacy and Security
8. Xie, Y., Lu, Z., Chang, R., Jiang, L., and Chen, W. (2017). An architecture based on TrustEnclaves to guarantee run-time security in embedded terminals. Science and Technology in Tsinghua, 22 (5).
9. In 2019a, Chen, G., Chen, S., Zhang, Y., Lin, Z., Xiao, Y., and Lai, T.-H. SgxPectre: Using speculative execution to steal intelligence secrets from SGX enclaves. in Stockholm, Sweden, at the Euro Sym on Security and Privacy. IEEE
10. Lai, T. H., Lin, Z., Zhang, Y., Xiao, Y., Chen, G., and Chen, S. (2019b). use speculative execution to steal Intel secrets from SGX enclaves. Proceedings of the Fourth IEEE European Security and Privacy Symposium. IEEE
11. Mazzeo, G., Coppolino, L., D'Antonio, S., and Romano, L. (2019). From the edge to the cloud: An extensive overview of hardware-assisted security. 100,055; Internet of Things, 6.
12. Perkusich, M. da Rocha, D. C. G. Valadares, K. C. Gorgonio, R. T. Pagno, and N. C. Will (2020). Client-side encryption and secure cloud storage using a trusted execution environment. Volume 1: CLOSER, Proceedings of the 10th International Conference on Cloud Computing and Services Science, pp 31–43. SciTePress and INSTICC
13. Chen, K., and Dai, H. (2017). OPTZ is a Trust-Zone Support-Based Hardware Isolation Architecture for Multiple Tasks. Pages 391–395 of the IEEE International Conference on Universal Computing and Communications (ISPA/IUCC) and IEEE International Symposium on Parallel and Distributed Processing with Applications.
14. Mendonca, P., Demesie Yalew, S., Haridi, S., Maguire, G. Q., and Correia, M. (2017). Truapp: A mobile app authenticity detection solution based on trust zones. In the IEEE 13th International Conference on Networking, Communications, and Wireless and Mobile Computing

Received: August 03, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

15. Esposito, A., Maisto, S., Rak, M., Ficco, M., Di Martino, B., and Nacchia, S. (2018). An overview of reference architectures, security, and interoperability for the Internet of Things. 1:99–112. Internet of Things.
16. Liu, P., Guan, L., Zhang, S., Yu, M., Cao, C., Xing, X., Ge, X., and Jaeger, T. (2019). establishing a reliable execution environment to stop cyber and physical space exploitation for arms. IEEE Secure and Reliable Computing Transactions, 16(3).
17. Intel (2016a). Developer Guide for Intel Software Guard Extensions. Intel Corporation.
18. Intel (2016b). Developer Reference for Intel Software Guard Extensions SDK for Linux OS. Intel Corporation.
19. Choi, C., Shin, Y., Kim, T., Kang, B. B., Han, D., Jain, P., Desai, S., Kim, S., Shih, M.-W., Lee, J., and Choi, C. (2016). An open platform for SGX research is called Open SGX. Proceedings of the Symposium on Network and Distributed System Security, San Diego, CA, USA. The Internet Society.
20. Chapuis, B., Garbinato, B., and V. Kulkarni (2017). location-based services that protect privacy by utilizing Intel SGSX. Published in New York, NY, USA, at the First International Workshop on Human-Centered Sensing, Networking, and Systems. ACM.
21. Hein, D., Winter, J., and Lesjak, C. (2015). Trustzone and security controller are examples of hardware-security systems for industrial IoT. at the IEEE Industrial Electronics Society's 41st Annual Conference.
22. Bowden, D., Li, D., Liu, J., Liang, X., Shetty, S., and Zhao, J. (2017). Healthcare systems are moving toward self-sovereignty and decentralized accountability. International Conference on Information and Communications Security Proceedings.
23. Maurice, C., Lipp, M., Gruss, D., Spreitzer, R., and Man-gard, S. (2016). Armageddon: Mobile device cache attacks. Austin, Texas, at the 25th USENIX Security Symposium. The USENIX Association.
24. McKeen, F., Shafi, H., Shanbhogue, V., Alexandrovich, I., Berenzon, A., Rozas, C. V., and Savagaonkar, U. R. (2013). Novel software models and instructions for isolated execution. Published in Tel-Aviv, Israel, at the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy. ACM.
25. He, W., Wu, H., Milutinovic, M., and Kanwal, M. (2016). An effective blockchain consensus protocol is proof of chance. SysTEX '16, New York, NY, USA: Proceedings of the First Workshop on System Software for Trusted Execution. The Computing Machinery Association.
26. Eisenbarth, T., Irazoqui, G., and Moghimi, A. (2017). CacheZoom: How cache assaults are strengthened by SGX. Pages 69–90, Taipei, Taiwan: Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems. Springer.
27. Sokolsky, O., Weimer, J., Lee, I., Phan, L. T. X., Nguyen, H., Ivanov, R., and Lee, I. (2018). LogSafe is an IoT device data logger that is both secure and scalable. Pages 141–152 of the

Received: August 03, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI).

28. Zhang (2017), Shi (2017), Ning (2017), and Shi (2017). Position paper: Difficulties with protecting environments with hardware assistance. New York, NY, USA: Proceedings of the Hardware and Architectural Support for Security and Privacy. ACM.
29. Kim, Kwangjo, and J. Park (2017). Tm-coin: Reliable TcB measurement management in IoT. during the Workshops of the IEEE International Conference on Pervasive Computing and Communications.
30. Varadarajan, S., Peters, T., Lal, R., Pappachan, P., and Kotz, D. (2018). BASTION-SGX: Trusted I/O on SGX through Architectural Support and Bluetooth. New York, NY, USA: Proceedings of the International Workshop on Hardware and Architectural Support for Security and Privacy. ACM
31. Johansen, D., Pettersen, R., and Johansen, H. D. (2017). Arm trustzone for safe edge computing. Proceedings of the Second International Conference on Big Data, Security, and the Internet of Things. SciTePress and INSTICC
32. Gomes, T., Tavares, A., Cabral, J., Pinto, S., and Pereira, J. (2017). Ltzvisor: The secret is Trustzone. The 29th Euromicro Conference on Real-Time Systems (ECRTS) proceedings.
33. Santos, N., and S. Pinto (2019). Arm trust zone demystification: An extensive survey. 51(6) ACM Comput. Surv.
34. Achemlal, M., Bouabdallah, A., and Sabt, M. (2015). The definition and characteristics of a trusted execution environment. Volume 1, pages 57–64, IEEE Trustcom/BigDataSE/ISPA, 2015.
35. Silva, F., Souza, A., Brito, A., Felber, P., and Sampaio, L. (2017). Data distribution for cloud-based apps that is safe and considerate of privacy. New York, New York, USA, Proceedings of the 10th International Conference on Utility and Cloud Computing, pages 47–56. ACM
36. Maurice, C., Schwarz, M., Weiser, S., Gruss, D., and Man-gard, S. (2017). Malware Guard Extension: Hide cache attacks with SGX. The 14th International Conference on Malware and Intrusion Detection and Vulnerability Assessment Proceedings, Bonn, Alemanha. Springer.
37. Lee, S., Kim, T., Shih, M.-W., and Peinado, M. (2017). T-SGX: Preventing attacks on enclave programs via regulated channels. San Diego, CA, USA: Proceedings of the Network and Distributed System Security Symposium. The Internet Society.
38. Barbosa, P., Silva, R., Brito, A., and Silva, L. (2018). Cloud computing data aggregation that considers security and privacy. Internet Services and Applications Journal, 9.
39. O. Surdu (2018). firmware updates for internet of things (IoT) devices that are safe and dependable. US 20180081666A1 is a patent.
40. Salvador, E. M., Brito, A. E. M., da Silva, M. S. L., and Valadares, D. C. G. (2018). utilizing FIWARE and Intel Software Guard Extensions (SGX) to distribute data securely. Proceedings of the IEEE Computers and Communications Symposium, Na-tal, RN, Brazil.

Received: August 03, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

41. In 2018, Wang, J., Jin, Y., Zhang, Y., and Hong, Z. Using Intel SGX for remote terminal and IoT to enable security-enhanced authentication. IEEE Integrated Circuits and Systems Computer-Aided Design Transactions, 37(1):88-96.
42. Bindschaedler, V., Tang, H., Gunter, C. A., Wang, W., Chen, G., Pan, X., Zhang, Y., and Wang, X. (2017). An understanding of memory side-channel dangers in SGX: A leaky cauldron on the dark continent. ACM SIGSAC Conference on Computer and Communications Security Proceedings, Dallas, Texas, USA, pp. 2421–2434. ACM.
43. Kurmus, A., Pietzuch, P., Weichbrodt, N., and Kapitza, R. (2016). AsyncShock: Taking advantage of synchronization errors in Intel SGX environments. In Heraklion, Greece, Proceedings of the European Symposium on Research in Computer Security, pp 440–457. The Springer

Received: August 03, 2025