International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-11 Issue-6, May 2022

Trusted Execution Environments for Internet of Things Devices

Abhilash Kayyidavazhiyil, Sheena Kaipacheri

Abstract*: A trusted execution Environment (TEE) could be a comfy place of a computer's essential processor that's designed to shield the most touchy information and operations. TEEs are utilized in an expansion of applications, which incorporates cell gadgets, price processing, and statistics safety. The usage of TEEs is becoming increasingly crucial because the amount of touchy records that are processed and stored electronically continues to develop. TEEs can help guard statistics from being accessed or changed with the resource of unauthorised customers, and can also assist ensure that facts aren't always compromised at some stage in transmission. TEEs typically applied the employment of specialized hardware that would offer a better degree of protection than software program-most effective solutions. Hardware-primarily based total TEEs can also offer better overall performance and power efficiency than software-handiest solutions. There are some particular TEE implementations to be had, which incorporates Intel's TXT, ARM's TrustZone, and Samsung's KNOX. Each of those implementations has its very personal strengths and weaknesses, so it's miles more crucial to pick the right TEE on your precise software. reckoning on execution environments are becoming an increasing number of necessities because the amount of touchy facts that's processed and stored electronically continues growing. TEEs can assist shield facts from being accessed or modified by means of way of unauthorized customers, and might also help make sure that records aren't compromised at some point of transmission. TEEs normally implemented the employment of specialized hardware, which will offer a far better degree of protection than software program-only answers. To research how this period has been implemented to the exceptional IoT eventualities, which normally address unique characteristics which incorporate device useful resource constraints, we allotted a scientific literature evaluation.

***Keywords*: Trusted Execution Environment, Internet of Things, Fog Computing, Security, Intel SGX.**

I. INTRODUCTION

The Internet of Things (IoT) term was used for the first time in 1999[1], [2], through Kevin Ashton, Whilst talking about the likelihood of a relationship between bodily gadgets and therefore the internet. RFID (Radio Frequency Identity) became sole amongst the foremost technologies utilized therein Time, permitting items tracking and identification, amongst other programs. IoT devices have very constrained resources, but those containing more computational power are called smart objects [3],[4]. The clever items and their interconnection enable many IoT programs in many domains, inclusive of logistics, transportation, enterprise, and healthcare. In view of that then, the propellant in lots of generation, and therefore the soaring of the several, has facilitated the charge discount of gadgets and accessories, tiger, better again, the agency and seminary concern. In the middle of analyzing the assorted possible scenario of Internet of Things packages. As long as the usage of those programmes is consistently growing, it comes to be essential for the maximum special possible options to standardise design architectures, conversation rules, with safety techniques to comfort the improvement of such solutions and improve the self-assurance of final customers [5]. The dearth of standardisation remains a mission, as well as, on those experiences, various organizations and free and open source clans have introduced middleware, agendas/frameworks, and different types of results. But, in that it is also not tangible, fashionable, properly definite and customary yet. As a consequence, corporations and human beings curious about the use of whichever answers have certain doubts and issues about the ones to pick or by what means to version a particular answer [3]. those concerns are even more so whilst the software program deals with sensitive records, which include Personal Identifiable Information (PII) or non-public Fitness Information (PHI), as its name for defense including need for smoothly-installed safety techniques. The previously mentioned plan means to supply a reliance on IoT shape (TIoTA) to carry out cosy IoT programs in step with it. The studied design architecture estimates cryptography, authorization, authentication, and trusted Execution Environments (TEEs) to build that one practicable [6]. Trusted Execution Environment additionally must offer a far off attestation mechanism which might show its trustworthiness for one third parties. Since 2010, Global Platform [6],has standardized the TEE specifications, which include the system architecture and APIs, such as TEE Client API, TEE Internal Core API, TEE Secure Element API.[7] The two main TEE technologies currently available in the market are ARM TrustZone [3] and Intel SGX.[4] Unlike ARM TrustZone, Intel SGX isn't compliant with the worldwide Platform specifications. For research how Trusted Execution Environment means to shield facts in fog/cloud-based Internet of Things applications, each one described great subsequent studies problems/troubles:

Manuscript received on 17 April 2022.
Revised Manuscript received on 03 May 2022.
Manuscript published on 30 May 2022.
* Correspondence Author
Abhilash Kayyidavazhiyil*, Research Scholar, Liverpool John Moore University, UK. E-mail: abhilashkv@yahoo.com
Sheena Kaipacheri , Senior Engineer, Digital 14.

● On which specific one are these proposals regarding the utilization of TEE in IoT applications?
● What type of Internet of Things quick fixes is Trusted Execution Environment recently active?

To reply to those complications, we completed a primary liberal arts assessment, seeking out associated papers during a number of the principle pc technological understanding clinical repositories (e.G., Scopus4, IEEE virtual Library5 and ACM digital Library6). To explore these, we used the subsequent key terms for search subjects: “TEEt” and “IOT” AND “safety”. We have given thought to high-quality precept TEE technologies to be had within the market: Intel SGX and ARM TrustZone. We have made the decision to look at 25 papers for each TEE era, this can be sufficient to urge a definition on the refined studies and find visions/instructions into manual after time exercises. Our major endowment are indexed as follows:

● A analysis on Trusted Execution Environment, exacted for safeguarding cloud/fog-based IoT applications, introducing relevant associated references;

A arguments about the provocations and purpose within the adoption of Trusted Execution Environment for Internet of Things applications with crucial analysis directions;

● A place to begin to hold out a scientific Literature Review regarding the research instructions/questions.

II. BACKGROUND

A. Arm Trustzone

TrustZone is the Arm TEE technology, which provides system-wide hardware isolation for trusted applications [20] .TrustZone era gives a simple infrastructure that allows SoC designers to select out quite some additives which could support definite functions inside one comfortable surroundings. The building design's vital intention acts as to permit the development of a configurable environment that provides the integrity as well as confidentiality of virtually every property likely shielded against precise assaults then maybe won't construct a bundle on safety answers since those aren't feasible with classic techniques. (ARM, 2009)

Alongside ARM TrustZone architecture, system/procedure may be inaccessible in analytical condition: a relaxed international and an everyday globe(Fig. 1) . The cosy global starts a reliable Operating System, answerable for separating with strolling relies on packages, imparting integrity and confidentiality to the system. The vulnerable globe operates an untrusted Operating System, commonly referred to as a wealthy OS, a typical OS inclusive of any Linux distribution. These states are signaled to all or any peripheral gadgets thru the machine bus, permitting them to form entry to manage decisions based at the device’s present day condition. The gear to blame for replacing the situation among the two status is understood as screen. TrustZone structure premises guarantee such isolation, offering admission to govern Memory divisions situated totally onto the trendy nation. This memory partitioning may be static or programmable at runtime.

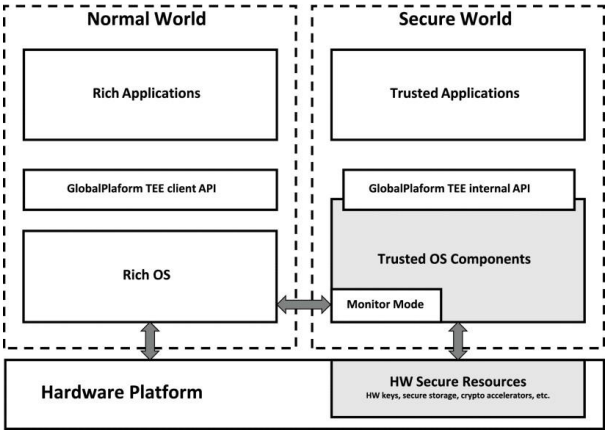

Fig.1. Trust Zone basic application architecture [8]

Trust Zone is used in billions of device applications to protect code and sensitive data in processes such as authentication, payment, and content protection [8].

B. Intel Software Guard Extensions (SGX)

Intel SGX may be a hardware-assisted Trusted Execution Environment (TEE) technology that protects code and data from disclosure or modification [9]. SGX is applied using the new Intel Processor education Set (ISA) referred to as Intel software protects Extensions (SGX). Intel software protect Extensions may be a set of CPU instructions that provide hardware-based safety functions to boost the protection of software programs. SGX permits packages to make enclaves, which are shielded from entry through other applications, including the package. SGX will be accustomed to protect sensitive information, including passwords, cryptographic keys, and company secrets and techniques. SGX also can be accustomed to guarding the execution of sensitive packages, like online banking packages.

SGX is implemented as a set of CPU instructions that allow software to create secure enclaves [10]. These enclaves are protected against access by other programs, including the OS. SGX provides variety of security measures, including:

• Confidentiality: Data within an enclave is confidential and can't be accessed by other programs, including the OS.
• Integrity: Data within an enclave is shielded from being modified by other programs, including the software.
• Authorization: Only authorised programs are allowed to access data within an enclave.

An SGX application is a Java application that uses the SGX SDK to create and manage enclave objects. An enclave is a secure area of memory that can be used to protect sensitive data from unauthorised access [11]. The SGX SDK provides a set of APIs that you can use to create and manage enclave objects [12], [13]. You can use the SGX SDK to make two sorts of enclave objects:

1. Protected enclave objects: Protected enclave objects are enclave objects which will be accessed only by the processes that created them.

2. Shared enclave objects: Shared enclave objects are enclave objects that may be accessed by any process that has been granted access to them.

Retrieval Number: 100.1/ijitee.F98850511622
DOI: 10.35940/ijitee.F9885.0511622
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

To create an enclave object, you initially have to create an SGX context. The SGX context provides the resources that you just have to create and manage enclave objects [12]. you'll use the SGX context to form and manage:

1. Protected enclave objects
2. Shared enclave objects
3. Enclave keys
4. Enclave certificates
5. SGX-specific system calls

III. COMPARISON BETWEEN ARM TRUSTZONE AND INTEL SGX

Table 1 represents a differentiation within the Intel SGX TEE and ARM TrustZone technologies' leading aspects. We observe that Intel SGX technology superposes the most specialties needed for the event of secure/protect applications beyond the requirement to rely on the software package or distinct highly privileged gears. Having said that, ARM TrustZone is able to bring a secured communication way to harmonious devices.

Table -I: Differentiation within the ARM TrustZone and Intel SGX TEE technologies

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

Even as Intel SGX technology dreams to supply a whole resolution with reference to the Central Processing Unit and reminiscence components' communique, ARM TrustZone shortfalls a problem able of supplying a relied on code measurement. A tool-precise secret's the concept of the comfortable storage and attestation mechanisms. In the aspect of a TPM, or some other component able to provide a really particular key and code dimension, it's feasible to supply those capabilities. Then again, Intel SGX technology is centered best at the Central Processing Unit and therefore the conversation alongside the memory, presenting no original characteristic to allow comfortable communique with input output devices, in evaluation to ARM TrustZone. It's vital to mix Intel SGX with other answers to permit the before-stated trusted communication, for instance, hypervisor-based totally relied on direction architectures [14].

IV. CHALLENGES

Using TEE brings some challenges that one must not ditch whilst developing strong and inexperienced solutions. However, the Intel SGX structure offers inexperienced mechanisms to create the protection of an utility's statistics. Aspect-channel assaults or contrary-engineering attacks don't seem to be within the structure's chance model. Hence, the SGX architecture is at risk of Spectre assaults. The manipulated waft of the region can be influenced to carry off commands mainly to observable cache kingdom adjustments, what type of a competitor can use to research mysteries and techniques from its registers or the memory of the enclave [15], [8]. Thread synchronization problems in enclaves also are addressed via techniques which include uses after free and time-of-test-to-time-of-use, permitting the aggressor to snatch the managed drift or skip enclave securities, authorization and verification, intervening threads, and pressing for division disasters in enclaves [16]. Some demanding situations to implement far flung attestation conventions to construct stable and scalable programs with SGX are mentioned via [17], [5].

Software builders may additionally anticipate that TEE is 100% secure, however it's not, and that they need to not forget insects with vulnerabilities in software and hardware additives. Additionally, they mustn't forget performance problems in both technologies. A vast range of views of the demanding situations concerning TEEs is discussed by Ning et al. [13]. Securing the firmware update process of IoT devices is paramount for any IoT ecosystem [12]. While renovating the firmware of any IoT gadget, a particular need to employ a steady/trustworthy and secure mechanism which permits it to be recompiled to a previous working prototype in case of update blunder. As observed, various contents are discovered, and lots of results can get pleasure from utilizing TEE. Blockchain might be a correlated subject that was discovered together with the solutions with both TrustZone and SGX , emphasizing the following attributes:

1. The data hashes are stored within the blockchain infrastructure.
2. Data are encrypted and stored in a very highly protected server or securely locally ;

Through, TEE is also a choice to maintain cryptographic keys and perform operations on sensitive statistics [13]. We recommend operating TEE for the foremost clinical quantities of the application, which could be discovered as a goal by way of the usage of involved adversaries without getting admission to permission.

V. RELATED WORK

Tasks had been completed exploring agreed with and safety problems within the IOT, featuring answers, and analyzing distinctive technology for those solutions. Based totally during this potential and wide examination vicinity, inspection and reportage were accomplished to guide those accepted as true with and safety works for sure. In terms of surveys, Aly et al. [16] highlights on lists and discusses works associated with safety intimidations and challenges normally terms. Other inspections, including Kouicem et al. (Kouicem et al., 2018), and Di Martino et al. [14] ,present extra well-known research and dialogue about distinct aspects of IoT, including interoperability and structure, making a parallel about how every observed painting pertains to think about and protection issues. But, none of that survey gift works associate to TEE and its operation on area/Fog answers.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Ankele et al. [12] supplied a survey of hardware assisted safety answers that concentrate on aspect computing eventualities. Distinctive sorts of hardware assisted protection technology are displayed in their paintings, together with the flexibility to use TEE. But, it is not always displayed as a precise analysis of tasks that open up Trusted Execution Environment technologies in their answers, which has its use inside and net of things situations. To the high-quality of information, at the moment, there is no written survey, outlining, or overview concerning the one-of-a-kind makes use of TEE for IoT applications.

VI. CONCLUSION

Dependent on Execution Environments are disbursed to brighten fact safety in awesome software program scenarios, considering fog, cloud, and facet computing. We finished a scientific literature evaluation to research how these technologies are meted out to defend information in Internet Of Things applications. For this, we described a protocol to effortlessly replicate this, have a glance at, and, in line with it, we selected fiftyeight works from the precept medical repositories, considering magazine and convention papers.

We provided a summary for every choice on paper and a dialogue approximately the principal disturbing situations associated with the usage of TEEs. Over and above, we additionally transferred on a concise dialogue concerning the principle studies subjects addressed with the help of TEEs utilization and their positive changes: comfortable and confidential statistics processing, comfortable repository, authentication, virtualization among others. As future works, we plan a scientific Literature overview specializing in all of the applicable papers published within the top meetings and journals.

REFERENCES

1. A. Gabbai, Kevin Ashton Describes the Internet of Things, Jan. 2015, [online] Available: https://bit.ly/2PvshSn.
2. K. Ashton, That ‘Internet of Things’ Thing, Jan. 2009, [online] Available: https://www.rfidjournal.com/articles/view?4986.
3. M. Henze, L. Hermerschmidt, D. Kerpen, R. Häußling, B. Rumpe and K. Wehrle, "A comprehensive approach to privacy in the cloud-based Internet of Things", Future Gener. Comput. Syst., vol. 56, pp. 701-718, Mar. 2016.
4. G. Kortuem, F. Kawsar, V. Sundramoorthy and D. Fitton, "Smart objects as building blocks for the Internet of Things", IEEE Internet Comput., vol. 14, no. 1, pp. 44-51, Jan. 2010.
5. S. Weagle, The Rise of IoT Botnet Threats and DDoS Attacks, Jan. 2019, [online] Available: https://bit.ly/2Qs4bIL.
6. E. Bertino, "Data security and privacy: Concepts approaches and research directions", Proc. IEEE 40th Annu. Comput. Softw. Appl. Conf. (COMPSAC), pp. 400-407, Jun. 2016.
7. R. van der Meulen, Gartner Says 8.4 Billion Connected ‘Things’ Will Be in Use in 2017 Up 31 Percent From 2016, Jan. 2019, [online] Available: https://gtnr.it/3snbJL9.
8. TruztZone—ARM Developer, Jan. 2021, [online] Available: https://developer.arm.com/technologies/trustzone.
9. Intel Software Guard Extensions (Intel SGX), Jan. 2021, [online] Available: https://software.intel.com/en-us/sgx.
10. S. W. Kim, C. Lee, M. Jeon, H. Y. Kwon, H. W. Lee and C. Yoo, "Secure device access for automotive software", Proc. Int. Conf. Connected Vehicles Expo (ICCVE), pp. 177-181, Dec. 2013.
11. R. Ankele and A. Simpson, "On the performance of a trustworthy remote entity in comparison to secure multi-party computation", Proc. Int. Conf. Trust Secur. Privacy Comput. Commun., pp. 1115-1122, 2017.
12. J. Wang, Z. Hong, Y. Zhang and Y. Jin, "Enabling security-enhanced attestation with intel SGX for remote terminal and IoT", IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 37, no. 1, pp. 88-96, Jan. 2018.
13. L. Zhang, D. Zhu, Z. Yang, L. Sun and M. Yang, "A survey of privacy protection techniques for mobile devices", J. Commun. Inf. Netw., vol. 1, no. 4, pp. 86-92, Dec. 2016.
14. Weiser, S. and Werner, M. (2017). SGXIO: Generic trusted I/O path for Intel SGX. In Proceedings of the 7th Conference on Data and Application Security and Privacy, CODASPY ’17, page 261–268, Scottsdale, AZ, USA. ACM.
15. Chen, G., Chen, S., Xiao, Y., Zhang, Y., Lin, Z., and Lai, T. H. (2019b). Stealing Intel secrets from SGX enclaves via speculative execution. In Proc. of the 4th IEEE European Symp. on Security and Privacy. IEEE.
16. Weichbrodt, N., Kurmus, A., Pietzuch, P., and Kapitza, R. (2016). AsyncShock: Exploiting synchronisation bugs in Intel SGX enclaves. In Proceedings of the European Symposium on Research in Computer Security, pages 440–457, Heraklion, Greece. Springer.
17. Beekman, J. G. and Porter, D. E. (2017). Challenges for scaling applications across enclaves. In Proceedings of the 2nd Workshop on System Software for Trusted Execution, New York, NY, USA. ACM.

AUTHORS PROFILE

Abhilash Kayyidavazhiyil, I have more than 23 years of experience in research and development in software industry. I did my b-tech in computer science and engineering from REC Calicut, after that did MSc in AI/ML from Liverpool Johnmoore university in UK. Also currently specialising in Robotics, cyber security and ai/ml.

Sheena Kaipacheri, I have more than 17 years of experience in software industry, mostly into embedded systems (mobile and STB). I have masters in computer science from MG University, Kottayam. Currently specialising in automation framework for secure mobile platform