Hindawi
Complexity
Volume 2020, Article ID 6612919, 9 pages
https://doi.org/10.1155/2020/6612919

Research Article

Establishment of Trust in Internet of Things by Integrating Trusted Platform Module: To Counter Cybersecurity Challenges

Mohammad Faisal[1], **Ikram Ali**[2], **Muhammad Sajjad Khan**[3], **Su Min Kim**[3], **and Junsu Kim**[3]

[1]*Department of CS & IT, University of Malakand, KPK 18800, Pakistan*
[2]*School of Automation Engineering, University of Electronic Science and Technology of China, Chengdu, China*
[3]*Department of Electronic Engineering, Korea Polytechnic University, Siheung, Republic of Korea*

Correspondence should be addressed to Junsu Kim; junsukim@kpu.ac.kr

Received 17 October 2020; Revised 25 November 2020; Accepted 11 December 2020; Published 21 December 2020

Academic Editor: M. Irfan Uddin

With the increasing day-to-day acceptance of IOT computing, the issues related to it are also getting more attention. The current IOT computing infrastructure brings some security challenges concerned with the users/customers and CSP. The users can store their confidential data at IOT storage and can access them anytime when they need. Lack of trust exists among IOT users and between IOT users and CSP. The prevention of this risk is a big research issue and it needs to be solved. There is a need for trusted IOT computing in recent times to provide trusted services. Here, we propose the integration of TPM in IOT computing to performs cryptographic operations and provide hardware-based security. In this domain, different schemes and methods have been proposed to build trust in IOT computing, but the suitable solution has not been presented by these schemes because these schemes lack in terms of some security services. A comparative study based on trusted computing schemes has also been presented in this paper along with different implementations of critical analysis. Our study is based on an overview of the main issues and summarizing the literature along with their strengths and limitations. In the end, we integrated the trusted platform module in the IOT architecture to establish the trust in IOT computing and to enhance the cybersecurity challenges and evaluated it with the help of mathematical/algorithms/graph theory/matrices and logical diagrams.

1. Introduction

With the rapid advancement in computing technologies, people who use smart devices can enjoy the ubiquitous facility of advanced technologies. IOT computing is one of the ubiquitous technologies and is defined as a technology, which provides network access to a pool of distributed shared computing resources such as software applications, storage services, and many other services needed by the customers on demand [1]. IOT computing offers the customers scalability and low-cost services and manages data based on the location-independent setup [2]. IOT computing now becomes worldwide in terms of services provided over the Internet and software applications [3]. The users can store their confidential data at IOT storage service and can access them anytime when they need. The IOT infrastructure is different from other distributive systems such as grid computing and cluster systems because the IOT computing environment is heterogeneously constructed and the IOT users belong to different local organizations having different security policies which join or leave the distributed resources dynamically which presents security problems [4]. The IOT computing brings some security challenges faced by customers between the IOT service provider (CSP) and its users. The users of the IOT are confused about their data stored on the IOT storage server that it is either secured or not and there is a chance for an unauthorized user to access it [3]. To prevent or minimize this risk is a big research issue. The IOT users want a system that provides security services such as confidentiality, authentication, integrity, and availability on time between CSP

and IOT users or among IOT users. Therefore, there is a need for a trusted relationship (based on security services) to provide trusted services among mentioned entities and to build the IOT environment trustable to everyone. The trust is defined as "*An entity can be trusted if it always behaves in the expected manner for the intended purpose*" [5, 6]. The trusted computing is an emerging technology developed and promoted by the trusted computing group (TCG) [7]. TCG consists of a group of industries that develop standards based on trusted computing techniques [8]. TCG implements one of its specifications, that is, a trusted platform module (TPM). The TPM chip is mounted on a platform motherboard and provides hardware-based security to the user's cryptographic operations. The TPM performs operations such as hardware encryption, signing, machine authentication, secure key storage, and attestation [8]. Encryption and signing are well-known techniques, but the TPM makes them stronger by storing keys in protected hardware storage [8]. Hardware-based TPM provides stronger security as compared to software TPM. Private Master Key is used by TPM to provide security for other pieces of information stored in the IOT computing system and TPM also stores hardware certificate to thwart attacks [9]. So TPM offers a root of trust for users in IOT computing because customers have full information about their identity [9]. In this context, different schemes have been presented along with their strength and weakness. TCG Best Practices Committee [10] proposed a hardware-based data location assurance solution (HDLAS) scheme to verify the geolocation of IOT user's data. The two building blocks of HDLAS are TPM and provable data possession (PDP). HDLAS does not need a third-party entity and provides the users with the preference option for data location. The trust has been established on CSP by the proposed scheme. Too many signaling messages and algorithms are involved in the communication process and make the computation lengthy and as a result, the communication among entities is affected. In Trusted Computing Group study [11], a mechanism is introduced to verify the information based on the geographic location of data. Only the attestation of geographic location information of data has been discussed but the integrity of data stored on the data center was not touched. Bare [6] stated the importance of trusted computing group (TCG) in IOT computing security and virtualization. Paladi [12] recommended DFIOT (data firewall IOT) technique for mobile devices to provide security at the client side. The rest of the paper is organized as follows. In Section 2, the architecture of TPM is illustrated along with a diagram. Different papers are reviewed along with their strengths and weakness in Section 3. In Section 4, paper works are critically analyzed. Section 5 presents the methodology of the TPM integration with IOT to establish trust in IOT computing and to enhance the cybersecurity challenges. The paper is concluded and future work has been proposed in Section 6.

2. Trusted Platform Module (TPM) Architecture

TCG is a group of industries (AMD, Hewlett-Packard, IBM, Intel, and Microsoft) aiming to create standards and specifications [7, 8]. TCG recommends the TPM specification in IOT computing to establish trust in the IOT environment. An international standard provides hardware-based security and is mounted as a chip in computing devices (laptops and desktop computers) and stores passwords, certificates, or encryption keys [8]. TPM guarantees protective computing in all environments such that TPM provides integrity because it measures the platform (computing device) status and ensures that the platform is trustable. TPM provides authentication which guarantees that the platform can prove that it is the intended entity. Attestation is also performed by TPM, which informs the remote party that a process or software on a platform is trustworthy and has not been compromised [13]. TPM chip contains 11 components shown in Figure 1. The detail of each component is beyond the scope of the paper but each was discussed briefly.

I/O: it controls the information flow over the communication lines and also performs encoding and decoding of the protocol [14]. Nonvolatile storage: it is a permanent memory used to store the owner authorization and permanent configurations as well as the endorsement key (EK) and storage root key (SRK) (nonmigratable keys) [14]. Platform Configuration Registers (PCRs): it is a 160-bit storage location used for integrity measurements and can be used in either nonvolatile or volatile memory. 16 PCRs are defined by TCG specification [5], 0–7 are kept for use of internal TPM, and 8–15 are used by the operating system and users' applications. Attestation Key Identity (AIK): this portion signs and authenticates the information legitimacy for external attestation purposes. Multiple clients on the same platform are accommodated by AIK, stored in outside data storage in the encrypted form [5, 14]. Program code: it is the core root of trust and contains firmware which is used to measure the devices of the platform [5, 14]. Execution engine: it depends on program code and performs execution as directed by the logic of program code [5]. Opt-in: it controls and maintains the states of the TPM chip by enabling activation and deactivation [5]. RSA engine: it uses the RSA algorithm and performs asymmetric encryption/decryption and signing operations [5]. Key generation: it uses protocol [15] based on the RSA algorithm to generate asymmetric encryption keys. SHA-1 engine: it is used to generate a hash which helps in digital signature creation [5]. Random Number Generator (RNG): it helps in key generation and nonce creation and makes stronger pass expression entropy [5].

3. Literature Review

TCG Best Practices Committee [10] proposed a hardware-based data location assurance solution (HDLAS) scheme to verify the geolocation of IOT user's data. The two building blocks of HDLAS are TPM and provable data possession (PDP). HDLAS scheme consists of three phases. TPM is a TCG security specification and has the ability to measure integrity and attest the remote party in IOT infrastructure. In HDLAS, TPM works along with a GPS receiver. PDP is a scheme used between client and server based on cryptographic operations. So due to this, IOT users are able to

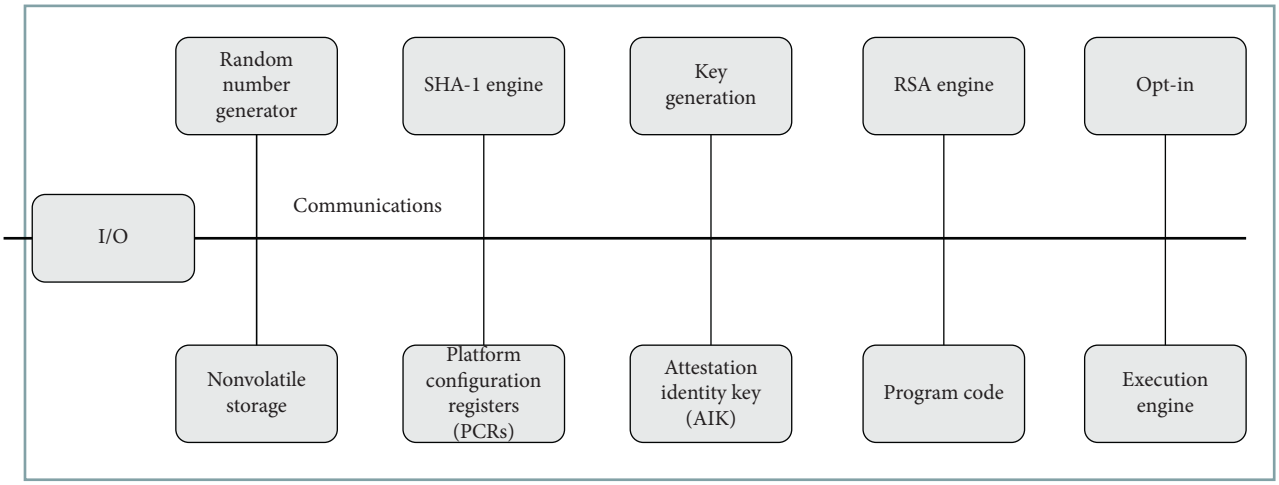

Figure 1: Trusted platform module (TPM) architecture [5].

obtain the correct information about the geolocation of their data stored in the storage server. The HDLAS can be applied to the existing system, that is, the Microsoft Azure; the existing provider of IOT storage used the proposed scheme. The attack model has also been discussed with regard to the IOT storage provider. HDLAS does not need a third-party entity and provides the users with the preference option for data location. The trust has been established on CSP by the proposed scheme. The proposed work is based on the comparative study of different previous techniques. But too many signaling messages and algorithms are involved in the communication process and make the computation lengthy and as a result, the communication among entities is affected. The simulation results have not been shown and discussed. The security services have not been analyzed on which trust is based. In V. et al.'s study [11], a mechanism is introduced to verify the information based on the geographic location of data. The technique is based on TPM and is used to attest location information of data remotely. Verifier, request processor, verification module, GPS device, and reply aggregator are the main entities of CSP and IOT environment used by the proposed approach. The third party has also been involved. During installation of TPM and GPS device, the TPM is set with coordinates of location according to the GPS device. When there is a need for attestation, the coordinates of location stored in TPM have been matched with location coordinates received from GPS at exact time. The attested information (based on matched/unmatched) is then forwarded to the verifier through different entities. The proposed work is carried out through the comparative study of different techniques. The security issues in relation to some security services have been mentioned. Only the attestation of geographic location information of data has been discussed but the integrity of data stored on data center was not touched. So due to this, there are threats to the integrity of stored data. Prototype is not given as whole work which is carried out descriptively. The simulation results have not been shown and discussed. Devi et al. [16] addressed the security of cloud computing infrastructure (CCI). CCI is based on virtualization. Authors recommend the extension to IOT computing that makes it trustable and suggest the use of TPM in virtualized environment to provide protection to key storage and integrity. Existing approaches and techniques such as virtualized hardware TPM, virtualized software TPM, para virtualization of TPM, and property-based virtualization of TPM have been analyzed by the authors. The software-based virtualized TPM offers interface to the hardware-based v-TPM and implementation of various operations is normally carried out by software-based v-TPM. The hardware-based v-TPM provides more security than software-based v-TPM. The para virtualization technique is achieved through hardware v-TPM and one hardware v-TPM is shared among some virtual machines. The property-based technique of virtualization of TPM provides updates of software and support migration of virtual machine. Some important and key research areas such as protocol for migration of virtual machine to v-TPM and attestation based on property-based technique have been discussed. The virtualization of TPM can reduce the cost. Every technique of v-TPM has been described along with their strengths and weak points. Only the structure and use of virtualized TPM have been discussed but how it is implemented has not been discussed. The security measures/services such as authentication, authorization, and confidentiality have not been clearly described. Bare [6] stated the importance of trusted computing group (TCG) in IOT computing security and virtualization. TCG provides standards, that is, IPM using trusted computing techniques for PC, laptop, mobile phones, storage, and networking security. TCG is used to address IOT security. TPM provides hardware-based security and is considered root of trust. Security features such as attestation, access control, measurements, logging, and reporting are provided by TPM. Credentials such as validation, endorsement, conformance, and platform identity, exchange of secure messages with TPM, and management of key are defined by TCG and used to establish trust chain. The authors analyze some approaches and techniques based on

TPM in IOT computing and virtualization along with functionalities of TPM, which are used to provide trust in IOT computing infrastructure and in virtualization. According to authors, these approaches and techniques do not present the required solution (i.e., to establish trust between IOT users and IOT service provider) and need fresh research work which extends or improves the specifications of TCG and secure IOT computing infrastructure and virtualization. Some future research work areas are pointed out with respect to TCG specifications in IOT computing security and virtualization. There is no new technique which has been discussed by the authors. This work is only based on analysis. No validation of the work is given; just the solution is descriptively given. Paladi [12] have analyzed the current existing technique for services of IOT storage such as Dropbox, which provides security at the server side based on encryption. It is still unsecure, because it does not provide encryption at client side, integrity of client platform attestation, and management of key based on hardware. In this paper, DFIOT (data firewall IOT) technique for mobile devices has been presented. This technique is used to provide security to the services of IOT storage and control the access to data in IOT storage. The problems (such as loss of data, data modification, and data leakage) found in Dropbox have been addressed by DFIOT. Proposed technique controls the data leakage at the server side by using encryption at the client side. DFIOT deploys TPM in mobile devices which provide management of keys. TPM also defines a protocol which shares or distributes keys among clients (users). The clients have mobile devices using ARM (advanced RISC machines) trust zone technology which manages keys based on hardware. Remote attestation is carried out by DFIOT to protect the leakage of data from malicious software at each client side. Software-based TPM (TPM emulator) has been used which provides less security as compared to hardware-based TPM. Full proof security and trust based on security services (authentication, access control, availability, and confidentiality) have also not been considered. TC Group [17] have analyzed the threats and security issues in IOT computing infrastructure (CCI). The CCI consists of some virtual machines (VMs) and uses virtualization technology. Virtualization is a technique by which one or more VMs are allocated to each client. The virtual machine monitor (VMM) also known as hypervisor is software based on kernel, which controls and manages the VMs. According to the authors, there are threats of attacks to security of VMM. The attacks are possible from inside and outside environment and therefore suggest some techniques and tools used to secure and protect the virtual IOT computing infrastructure (VCCI) from attacks. The tools and techniques are intrusion detection tools, virtual trusted platform module, virtual firewalls, encryption and management of keys, mechanisms used for access control, and trusted virtual domains (TVDs). The protection of VCCI is possible if the mentioned techniques and tools are carried out completely. The work of this paper addressed very important critical security issues in current VCCI and also explored future research areas which belong to security issues from working and governance point of view in IOT computing. All of the suggestions have been discussed conceptually but their validation results have not been discussed and have not been shown. Rivest et al. [18] have analyzed problem in virtual infrastructure due to the provisioning based on dynamic management of security. Dynamic infrastructure trusted bootstrapping protocol (DITBP) has been introduced to make trust between two machines. The DITBP is designed to improve advanced architecture such as the Dynamic Access Control Infrastructure (DACI). The proposed approach consists of those mechanisms and infrastructure that is based on TCG and TCG provides TPM. TPM provides hardware security and root of trust. TPM generates pair keys and handles exchange of keys. TCP (transmission control protocol) and TLS (transport layer security) are utilized by DITBP for communication between nodes. The process of DITBP is event driven, that is, consisting of request and response. The components involved in the bootstrapping process which are domain authentication server (DAS) produce trust for proxy type domain, bootstrap initiator (BI) is an application that makes sure of the position of the remote machine when it is transferred, bootstrap requester (BREQ) is an client type application used to provision infrastructure and executes on the remote machine, and bootstrap responder (BRES) is a server type application used to authenticate the machine to a distant client machine and allows the client to bootstrap the machine. The proposed technique is based on the comparative study of different frameworks and provides foundation of future research work for those who want to do more work in security of dynamic establishment infrastructure through trusted bootstrapping protocol. But the proposed work still missed some requirements for implementation, that is, does not show simulation results. The DITBP does not explain the security services on which TPM is based.

Noman and Adams [19] analyzed the need of establishing trust in the virtualized IOT platform. An approach based on a trusted service domain (TSD) has been proposed to establish trust on the virtualization platform of IOT. TSD is considered the root of trust for the IOT virtualization environment. TSD is based on TPM, which provides hardware security and generates keys. Extended trusted chain for TSD security and TSD is associated with TPM based on the generation of keys to control user domains or virtual machines (VMs). TSD offers trusted services to multiple user domains based on independent functional domain specifically. The scheme based on TSD has been presented to protect data and make safe communication among domains. The migration of user domains based on TSD is also presented. The proposed mechanism is based on the comparative study of previous models, that is, private virtual infrastructure (PVI), trusted virtual environment module (TVEM), and so on. The communication among TSD, Admin Dom, and user Dom has clearly been discussed and achieved some good results as compared to existing schemes. TSD provides flexibility and scalability. Future research areas have been mentioned by the proposed work. In the proposed work, the established trust in the virtualized

IOT platform has not been explained clearly. The functionalities of TSD and TPM are the same; then why does TPM use directly instead of TSD? The architecture is composed of too many components, that is, TPM, VMM, Admin doom, and TSD, and user domains can affect the performance of IOT platform services. The security services have not been explained. In Vaish et al.'s study [20], the technology that is trusted in the IOT computing environment is recommended. The technology is provided by TCG (trusted computing group), that is, the trusted computing platform (TCP) making the system, that is, data and applications, cryptographically secure. The TCP is based on trusted platform support services (TSS) and TSS is a part of TCP. TSS in turn depends upon the trusted platform module (TPM) and provides hardware-based security. The TSS acts as a bridge between upper layer applications and lower layer hardware. TPM can contact TSS and provide security services (authentication and access control) via TSS. TPM chip is mounted on the motherboard of a PC for the purpose of authenticating hardware and offers the trusted information about the internal state of the system. The encryption keys, certificates, and passwords which help in maintaining data privacy are stored by TPM. It also protects unencrypted keys from software-based attack. The strength of the work is that trusted computing technology specifications are deployed in IOT computing environment. Security provided by hardware (TPM) is stronger than security provided by software. The proposed strategy explained security services such as access control, protection of data, and authentication. The authors just discussed the work conceptually but how it is implemented has not been shown. Simulation results have not been given and analyzed. Wan et al. [21] have analyzed the platform and virtualization of IOT computing, reference model related to security of IOT computing, TPM, trusted network access, and architecture of network platform that is trusted. For trusted network platform architecture, TNA (trusted network access) and TPM are necessary. TPM is installed on both IOT client terminal and IOT server systems to produce trusted relations between the IOT client and IOT server. Clients trusts in server and server trusts in clients. Due to this, the services belonging to IOT will be offered to clients by server. The architecture of trusted IOT client terminal system and trusted IOT server is also explained. TPM is arranged in IOT client terminal system to confirm the identity of IOT server. Similarly, the TPM is used in IOT server to prove the identity of IOT client terminal. The trusted network platform approach protects the clients of IOT and its relevant services and provides system of measurement. It also offers the trustworthiness of identity between server and client. The given approach based on TPM allows TNA make the IOT computing environment secure. The proposed approach not only provides security between client and server but also provides the security service such as integrity of IOT service. The given work is too short and not enough to understand. Security services such as authentication, confidentiality, access control, nonrepudiation, and its mechanisms have not been discussed. The effects on IOT client system and IOT server have not been discussed. Achemlal et al. [22] analyzed the challenges (such as scalability of platform, software up gradation and licensing, recovery, availability, accessibility, and system security) faced to CSP and on the basis of these challenges, efficient and secure educational platform (ESEP) has been proposed. ESEP is mainly based on security of data stored on IOT. Some security techniques and tools such as TPM, v-TPM, trusted virtual domain (TVD), intrusion detection system (IDS), and security as a service (SE-CaaS) have been recommended by author. The authors claim that when a user signs SLA (service level agreement) with CSP, then this user becomes trusted user such as Microsoft Live@edu. HRMS, LMS, and untrusted users are general public registered users who use CSP online. The layer based on virtualization has also been secured using mention techniques and tools. The physical layer is secured by TPM trusted execution technology (TXT). The security as a service is achieved through software that is bit locker enabled by TPM to protect data storage through cryptographic operations. The authors discussed reason of lack of confidence on CSP by educational organizations. ESEP is based on all in one. But ESEP has been discussed conceptually; that is, no prototype has been given in the proposed work. Simulation results have not been given upon discussion and analysis is based on the simulation but results are not given. The full proof security and trust based on security services have also not been analyzed. Shin et al. [23] proposed an approach used to establish trust in IOT computing environment by integrating trusted computing platform (TCP). The TCP based on TPM and TPM on behalf of TCP provides some security services such as confidentiality, integrity, and authentication in IOT computing infrastructure. The proposed approach uses stream cipher algorithm; that is, RC4 (R. Cipher-4) offers the mentioned security services. RC4 algorithm is comprised of two parts such as key scheduling algorithm (KSA) and pseudorandom generator algorithm (PRGA) and encryption/decryption process is carried out in two phases. RC4 algorithm performs the encryption of data in a very short interval of time, that is, in nanoseconds, due to which, computation time is reduced and better performance is achieved. The proposed approach is based on security services. On the other hand, the encryption process which takes short time, that is, nanoseconds, can affect the security of the IOT computing system. The encryption process time is directly proportional to the size of the data. Brohi et al. [24] highlighted the problem faced currently by mobile nodes when verifying or updating their data on the IOT storage server at the same time. The provable data possession (PDP) is the existing scheme used by mobile node in IOT environment. The mobile nodes are resource constrained, that is, low in processing and small in storage, and therefore cannot support computation workload and burden of storage services in IOT environment. The author recommends the use of TCG specification such as TPM and modifies the PDP scheme, in which trusted-third-party agent (TPA) has been introduced. The TPA performs most of the computations of end user (mobile device) on behalf of the end user/mobile node. First of all, end user and TPA authenticate each other and build a secure path. Then Daffier-Hellman protocol is used to exchange symmetric keys between end user and TPA

Table 1: Critical evaluation of the schemes discussed in the literature.

Lit. ref.	Technique used	Focus area	Pros	Cons
[10]	Hardware-based data location assurance solution (HDLAS) scheme using TPM and PDP	To enable the IOT users to verify the geographic location of their data stored in any data center accurately	HDLAS can be applied to the existing system and does not need a third party	Too many signaling messages and algorithms still are involved in the communication process
[11]	TPM-based scheme for remote attestation	To allow the clients of IOT computing to verify the information based on the geographic location of their data stored in any data center accurately	Simple architecture to learn and take care of regulatory concerns for the IOT computing environment	Still exist threats to the integrity of data. Proposed work is carried out conceptually; that is, simulation results have not been shown and analyzed
[16]	Use of TPM virtualization in IOT computing	To secure and establish trust in the IOT computing environment by using the virtualization of TPM	Point out key research areas and virtualization of TPM can reduce the cost and offer the flexibility of the platform	IOT security is not limited to the virtualization of TPM. Proposed work needs to be simulated on the basis of security services
[6]	Context and motivations for specifications of TCG based on TPM	To establish trust between the IOT service provider and IOT user by deploying TPM in CCI	TCG specifications are not mature up till now to secure IOT computing and virtualization. Future research work areas	The author does not have their own technique. Analyzed but without validation
[12]	Data firewall IOT (DFIOT) technique based on TPM	To provide security at the server and client side and security to the services of IOT storage and control the access to data in IOT storage	Remote attestation protects the leakage of data from malicious software at each client side	Software-based TPM (TPM emulator) provides less security as compared to hardware-based TPM and full proof security is based on security services
[17]	Tools and techniques to secure virtual IOT computing infrastructure (VCCI)	To make the security of VMMs strong and protect them from inside or outside attackers in VCCI	Pick up an immensely important security issue in current VCCI and explore future research areas from a working and governance point of view	CCI security is not only limited to virtualization. There are other layers that need security. Proposed work needs to be simulated on the basis of security services
[18]	Light-weight trusted scheme, that is, dynamic infrastructure trusted bootstrapping protocol (DITBP) based on TPM	To establish trust between two machines in the IOT computing infrastructure	Integrate many solutions in one infrastructure which provides better effects. Provide the foundation of future research areas	Trust is also necessary between IOT users and CSP. Proposed work needs to be simulated and analyzed on the basis of security services
[19]	Scheme based on trusted service domain (TSD).	To deliver services for multiple user domains that are trusted on the virtualization platform of the IOT environment.	Have good results as compared to existing schemes, that is, in terms of flexibility and scalability. Mentioned future research areas.	Functionalities of TSD and TPM are the same; then why does TPM use directly instead of TSD.
[20]	Trusted computing platform (TCP) using trusted platform support services (TSS) based on TPM	To make the system, that is, data and applications, cryptographically secure and provide hardware-based security	Make the CSP trustable to clients. Security provided by hardware TPM is stronger than the security provided by software TPM	Proposed work needs to be simulated and analyzed on the basis of security services for IOT computing infrastructure
[21]	IOT computing security scheme, that is, trusted network platform architecture based on virtualization	To produce trusted relations between the IOT client and IOT server and also ensure the integrity of IOT services	Establish trust between server and client. Provide the security service such as integrity of IOT service	Given work is too short and not enough to understand. Proposed work needs to be simulated and analyzed on the basis of security services for the IOT computing environment
[22]	Efficient and secure educational platform (ESEP) scheme	To make CSP trustable to educational organizations by providing features such as scalability, flexibility, security, availability, recovery, software on demand, and omnipresent accessibility of IOT computing	Bit-locker software enabled by TPM provides better security as compared to others. Explore many key research areas of IOT computing. ESEP is based on all in one	The prototype of ESEP is not given. It is difficult to implement ESEP because it works on more than one feature. Proposed work needs to be simulated and analyzed on the basis of security services

Table 1: Continued.

Lit. ref.	Technique used	Focus area	Pros	Cons
[23]	Integration of a trusted computing platform (TCP) in the IOT computing environment	To establish trust by integrating a trusted computing platform in the IOT computing environment to provide security services such as confidentiality, integrity, and authentication	Encryption of data is performed in a very short interval of time, that is, nanoseconds, due to which, computation time is reduced and better performance is achieved. Security services is carried out by the RC4	The encryption process takes short time, that is, nanoseconds, which can affect the security of the IOT computing system. The encryption process time is directly proportional to the size of the data
[24]	Provable data possession scheme together with trusted computing technology for mobile nodes in IOT computing environment	To allow the resource-constrained devices such as mobile nodes to use the services of IOT computing without any trouble and reduce the workload on mobile nodes by using TPM chip mounted on client mobile node	The workload is minimized by TPM. Clients can verify and update data unlimitedly at the same time. TPM chip avoids man in the middle attack. CSP cannot understand client data	One security service is left, that is, availability. The prototype of the proposed system is necessary to show the performance of the scheme which has not been discussed
[25]	Integration of trusted computing with IOT computing environment	To build trust by integrating a trusted computing platform with an IOT computing environment to provide security services such as confidentiality, integrity, and authentication	Security services such as confidentiality, integrity, and authentication can build trust up to some extent in the IOT computing environment. The origin of the users can also be traced	Availability is also very important which has not been discussed. The proposed method has not been validated and implemented because the prototype of the proposed approach along with simulation results is not discussed

and encrypt data files. Merle hash tree (MHT) is used to show the integrity of the data blocks and update data dynamically. Bilinear map is a signature work together with MHT to minimize the computation workload at mobile node and storage services of data at IOT server. With the integration of trusted computing technology, the TPM chip is mounted at client mobile node to generate and store secrete keys and random numbers to avoid man in middle attack. The file transferred from TPA to CSP is encrypted and is not known by CSP. Whole work is based on the comparative study of the existing and previous schemes. Due to TPM chip, TPA verifies the accurateness, integrity, and privacy of data and minimizes the burden of processing workload and storage services on client/mobile device. The proposed scheme is as simple as three entities which are involved such as mobile node, TPA, and CSP. The three main security services such as privacy, integrity, and authentication are carried out. But one security service is left, that is, availability. Prototype of the proposed system is necessary to show that the performance of the scheme has not been discussed. Membrey et al. and Chang et al. [25, 26] addressed the requirements of security for IOT computing systems. The requirements are based on trusted computing in IOT computing. In this paper, a method to establish trust in IOT computing environment through the integration of trusted computing platform (TCP) which is based on TPM is presented. TPM is considered as root of trust of users. The proposed method is based on four main mechanisms. With TCP, everyone who wants to access IOT computing systems must be authenticated. With TCP, unauthorized access to IOT computing services and resources is impossible and protected [27–30]. With TCP, the security of data is also improved because session keys and random numbers are created. TPM generates encryption key and session key due to which, the data stored in computer are encrypted. With TCP, the IOT computing systems can trace the users' origin through a mechanism based on user personal key which proves the user identity and the mechanism is kept in hardware such as TPM and BIOS. If security services such as confidentiality, integrity, and authentication are achieved correctly, this can build trust up to some extent in IOT computing environment. The security service, that is, availability, is also very important and has not been discussed. The proposed method has not been implemented or validated because prototype of the proposed approach is not given and simulation results are not given often analysis is based on simulation and not given in literature by the authors [29, 30].

4. Critical Evaluation

In Table 1, we critically evaluate the techniques used and the platform of installation with its respective pros and cons.

5. Methodology

We evaluate our scheme with the help of mathematical algorithms and logical diagram as shown as follows. In Algorithm 1, we elaborated the integration of trusted platform computing in IOT architecture in a stepwise manner.

5.1. Logical Diagram. With the help of graph theory, we evaluated the integration of TPM with IOT architecture to

```
START: I == 0, WHILE I == 1 {
IF RNG
THEN (Switch (SHA_1): Switch (KG): Switch (RSA); Switch (Opt) :}
ELSE IF
{NVS
THEN (Switch (PCR): Switch (AIK); Switch (PC); Switch (EE) ;}
I++
```

Algorithm 1: (SHA, KG, RSA, PCR, AIK, PC, EE).

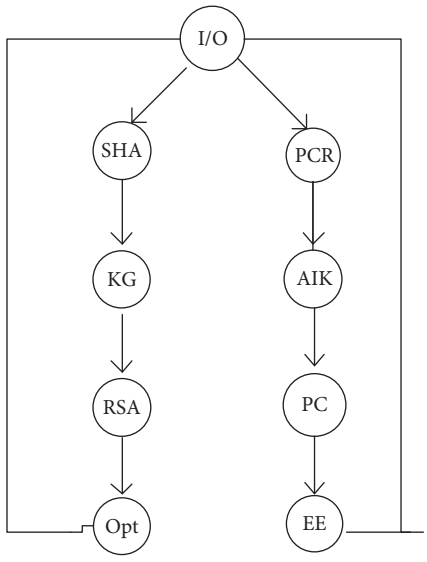

Figure 2: Logical diagram.

$$M1 = \begin{array}{c} \\ \text{PCR} \\ \text{AIK} \\ \text{PC} \\ \text{EE} \end{array} \begin{array}{c} \begin{array}{cccc} \text{SHA} & \text{KG} & \text{RSA} & \text{Opt} \end{array} \\ \begin{bmatrix} 0 & a12 & a13 & a14 \\ b21 & 0 & b23 & b24 \\ c31 & c32 & 0 & c34 \\ d41 & d42 & d43 & 0 \end{bmatrix} \end{array}$$

Figure 3: Mathematical analysis with respect to matrices.

enhance the trust and counter cybersecurity challenges as shown in Figure 2.

5.2. Mathematical Analysis of the Scheme. After evaluating by algorithms and logical diagram, the result of TPM integration in IOT architecture is analyzed with the help of matrices. The right diagonal shows that if there is a security lapse, then the right diagonal elements will become off as shown in Figure 3. Else if the diagonal elements are not off, then it will successfully integrate the trusted platform module in the IOT architecture.

6. Conclusions and Future Work

IOT computing technology is one of the ubiquitous technologies which provides network access to a pool of distributed shared computing resources such as software applications, storage services, and many other services along with scalability and low-cost services and manages data without location limits independently. The IOT computing brings some security challenges faced by customers between IOT service provider (CSP) and its users and among users and this is the lack of trust on CSP. Here, we suggest the use of TPM in IOT computing systems to make it trustable. All operations such as hardware encryption, signing, machine authentication, secure key storage, and attestation are performed by TPM. In this paper, in this context, different techniques and methods concerned with the integration of TCG specification (TPM) in IOT computing to provide trusted IOT computing are studied but the suitable solution has not been presented because these techniques have deficiencies in terms of security services (confidentiality, integrity, authentication, and availability). Trust among IOT users and trust between IOT users and CSP are the main focus of this study. The schemes and techniques based on trusted IOT computing are comparatively studied; one approach offers authentication and integrity but leaves confidentiality and availability; others do the reverse of this. Some different emerging research areas in the field of trusted IOT computing are presented by this research. The next work is based on the integration and improvement of TCG security standard (TPM) in IOT computing to achieve security services as mentioned because trusted computing is based on security services. The review of different schemes based on trusted IOT computing has not presented the appropriate solution, so we are going to plan the technique to provide the optimized solution in comparison with the present state of the art techniques.

Data Availability

The data supporting the findings of this study are available within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding the present study.

Acknowledgments

This work was supported in part by the MIST (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2020-

2018-0-01426) supervised by the IITP (Institute for Information and Communication Technology Planning & Evaluation) and in part by the National Research Foundation (NRF) funded by the Korean Government (MIST) (no. 2019R1F1A1059125).

References

[1] J. Li, M. Nazir Jan, and M. Faisal, "Big data, scientific programming, and its role in internet of industrial things: a decision support system," *Scientific Programming*, vol. 2020, Article ID 8850096, 7 pages, 2020.

[2] X. Liao, M. Faisal, Q. Q. Chang, and A. Ali, "Evaluating the role of big data in IIOT-industrial internet of things for executing ranks using the analytic network process approach," *Scientific Programming*, vol. 2020, Article ID 8859454, 7 pages, 2020.

[3] M. Faisal, S. Abbas, H. U. Rahman, M. Z. Khan, and A. U. Rahman, "An analysis of DDoS attacks on the instant messengers," *Security and Communication Networks*, vol. 2019, Article ID 1751285, 8 pages, 2019.

[4] I. Ali, M. Faisal, and S. Abbas, "A survey on lightweight Authentication schemes in vertical handoff," *International Journal of Cooperative Information Systems*, vol. 26, no. 1, Article ID 1630001, 2017.

[5] S. L. M. Deepthi, G. Yamini, P. Srinivasarao, and K. Sivaramakrishna, "A novel and cost-effective approach for privacy," *International Journal of Advanced Computer Communications and Control*, vol. 2, no. 3, 2014.

[6] J. C. Bare, *Attestation and Trusted Computing-CSEP 590: Practical Aspects of Modern Cryptography*, The Association for Computing Machiner, New York, NY, USA, 2006.

[7] S. Goyal and R. Mathew, "Security issues in IOT computing," in *Proceedings of the International Conference on Computer Networks, Big Data and IoT*, Springer, Madurai, India, December 2020.

[8] C. Kumari, G. Singh, G. Singh, and R. Singh Batth, "Security issues and challenges in IOT computing: a mirror review," in *Proceedings of the 2019 International Conference on Computational Intelligence and Knowledge Economy*, Dubai, UAE, December 2019.

[9] A. K. Sen and P. K. Tiwari, "Security issues and solutions in IOT computing," *IOSR Journal of Computer Engineering*, vol. 19, pp. 67–72, 2020.

[10] TCG Best Practices Committee, *Design, Implementation, and Usage Principles Version 2.0*, Trusted Computing Group, Beaverton, OR, USA, 2005.

[11] Trusted Computing Group (TCG), *IOT Computing and Security–A Natural Match*, Trusted Computing Group, Beaverton, OR, USA, 2010.

[12] N. Paladi, *Trusted Computing and Secure Virtualization in IOT Computing*, Swedish Institute of Computer Science Secure Systems Group, Stockolm, Sweden, 2012.

[13] P. Mell and T. Gance, "The nistdenition of IOT computing," Tech. Rep., National Institute of Standards and Technology, Gaithersburg, ML, USA, 2011.

[14] E. D. Canedo, R. T. Junior, and R. O. Albuquerque, "Trust model for reliable file exchange in IOT computing," *International Journal of Computer Science and Information Technology (IJCSIT)*, vol. 4, no. 1, 2012.

[15] X. Wu, "A new trust model in cloud computing environments," *International Journal of Hybrid Information Technology*, vol. 8, no. 3, pp. 177–184, 2015.

[16] M. R. Devi, S. P. Balamurugan, and K. Thanushkodi, "The trusted computing exemplary with astonishing security for IOT computing," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 11, no. 1, 2011.

[17] TC Group, "TCG specification, architecture overview, revision 1.4," Tech. Rep., Trusted Computing Group, Beaverton, OR, USA, 2007.

[18] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[19] A. Noman and C. Adams, "Hardware-Based DLAS: achieving geo-location guarantees for IOT data using TPM and provable data possession," in *Proceedings of the 17th International Conference on Computer and Information Techology*, pp. 280–285, Dhaka, Bangladesh, December 2014.

[20] A. Vaish, A. Kushwaha, R. Das, and C. Sharma, "Data location verification in IOT computing," *International Journal of Computer Applications (0975–8887)*, vol. 68, no. 12, pp. 23–26, 2013.

[21] X. Wan, Z. T. Xiao, and Y. Ren, "Building trust into IOT computing using virtualization of TPM," in *Proceedings of the Fourth International Conference on Multimedia Information Networking and Security*, pp. 59–63, Irvine, CF, USA, December 2012.

[22] M. Achemlal, S. Gharout, and C. Gaber, "Trusted platform module as an enabler for security in IOT computing," in *Proceedings of the Network and Information Systems*, La Rochelle, France, May 2011.

[23] J. Shin, Y. Kim, W. Park, and C. Park, "DFIOT: a TPM-based secure data access control method of IOT storage in mobile devices," in *Proceedings of the IEEE 4th International Conference on IOT Computing Technology and Science*, pp. 551–556, Taipei, Taiwan, December 2012.

[24] S. N. Brohi, M. A. Bamiah, M. N. Brohi, and R. Kamran, "Identifying and analyzing security threats to virtualized IOT computing infrastructures," in *Proceedings of the IEEE 2012 International of IOT Computing, Technologies, Applications and Management*, pp. 151–155, Dubai, UAE, December 2012.

[25] P. Membrey, K. C. C. Chan, C. Ngo, Y. Demchenko, and C. d. Laat, "Trusted virtual infrastructure bootstrapping for on demand services," in *Proceedings of the IEEE Seventh International Conference on Availability, Reliability and Security*, pp. 350–357, Prague, Czech Republic, August 2012.

[26] D. Chang, X. Chu, Y. Qin, and D. Feng, "TSD: a flexible root of trust for the IOT," in *Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 119–126, Liverpool, UK, June 2012.

[27] Z. Shen, L. Li, F. Yan, and X. Wu, "IOT computing system based on trusted computing platform," in *Proceedings of the IEEE International Conference on Intelligent Computation Technology and Automation*, pp. 942–945, Changsha, China, May 2010.

[28] Y. Liu, L. Tan, and Q. Yi, "A trusted network platform architecture scheme on IOTing computing model," in *Proceedings of the IEEE International Conference on Computer Science and Information Processing (CSIP)*, pp. 890–892, Xi'an, China, August 2012.

[29] S. Abbas, M. Faisal, H. Ur Rahman, M. Z. Khan, M. Merabti, and A. u. R. Khan, "Masquerading attacks detection in mobile ad hoc networks," *IEEE Access*, vol. 6, pp. 55013–55025, 2018.

[30] S. N. Brohi, M. A. Bamiah, S. Chuprat, and J. I. A. Manan, "Towards an efficient and secure educational platform on IOT infrastructure," in *Proceedings of the IEEE 2012 International of IOT Computing,Technologies*, pp. 145–150, Palermo, Italy, July 2012.