Centralized Accessibility of VM for Distributed Trusted Cloud Computing

1st Ubaidullah alias Kashif
Department of Computer Science
The Shaikh Ayaz University
Shikarpur, Sindh, Pakistan
kashif@saus.edu.pk

2nd Zulfiqar Ali Memon
Department of Computer Science
National University of Computer and Emerging Sciences (FAST-NUCES),
Karachi, Pakistan.
zulfiqar.memon@nu.edu.pk

3rd Sajid Ahmed Ghanghro
Department of Computer Science
Shah Abdul Latif University
Khairpur.
Department of Information and Computer Science, Saitama University, Japan.
sajid.ghanghro@salu.edu.pk,

4th Wajid Ahmed Channa
Department of Computer Science
Sukkur IBA University
wajidahmed.msse14@iba-suk.edu.pk

5th Abdullah Soomro
Department of Computer Science
Islamia University, Bahawalpur
abdullah.soomro@iub.edu.pk

2023 4th International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) | 979-8-3503-3531-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICOMET57998.2023.10099351

Abstract— **Cloud computing platforms constructed on Trusted Computing Technology are commonly referred to as trusted cloud computing. The core component of this technology is known as Trusted Platform Module (TPM). Its specifications are given by the consortium known as Trusted Computing Group (TCG). Though TPM is an immovable module and is fixed inside any computer, yet its credentials can be shared with other devices. This paper presents the accessibility model for Virtual Machine (VM) of a distributed trust protocol which is based on TPM, through which consumer's credentials are shared to other trusted devices. These credentials essentially describe the integrity of VM.**

Keywords— Trusted Cloud computing, Distributed Trust Models, Virtual machine integrity

I. Introduction

Cloud computing is a new way of outsourcing IT services as an online service. Although varying to the field of distributed, cluster or grid computing the use of the Internet in cloud computing separates it from the cluster and the grid computation. As per the terminology of cloud computing implies, the word cloud refers to the Internet that rawhides the basic enigmas of cloud computing users and conveys the seamless thinking of accepting Information Communication Technology (ICT) computation facilities from the cloud service provider (CSP). The domain of cloud computing includes three components namely Cloud Infrastructure, Cloud Provider and Cloud Consumer. Cloud computing services are used in other forms of conveyance such as Software as a Service, Platform as a Service and infrastructure as a service. According the definition of SaaS, code and databases furnished to several clients. In PaaS, software development platform is provided. IaaS allows the consumer to produce a complete and fully functional virtual machine with network capability, data storage devices, CPU or GPU processing, run time memory and almost all other resources needed for integration.

Cloud services can be used likewise we use utilities in our daily life i.e. pay what you use. IaaS model is a fundamental layer for the cloud environment. At this layer computing resources are designed for virtualization purposes, in order to achieve widespread distribution and deployment. Due to high deployment, there is a high risk of security attacks and it is very difficult for a cloud buyer to rely on such a multi-tenant site. Cloud computing and IaaS security issues such as data security and privacy, trust, multiple tenants, damage, and data leaks, malicious VM etc are shown in [2] and [3]. Caring these issues it is very difficult for the consumer to rely on the infrastructure provided to the consumer. User stores data in bought machines (VM) swung on the provider facet for processing and other purposes. It is important to examine the cloud equipment for privateness and integrity before, after and at some stage in VM implementation. The literature reviewed for this motive conveys the clean impact that there may be a loss of such structures that permit the user to discover a VM controlled with integrity and privateness. In the IaaS framework all environmental safety measures are done via way of means of the provider, so the user ought to depend now no longer best on his or her infrastructure however additionally on his or her personal countermeasures. Here the query arises of believe withinside the protection supplied via way of means of the issuer. The visible infrastructure provided to the user is below the bodily manage of the provider and may be accessed via way of means of the provider through a unique hypervisor domain. In the [4],[5],[6] and [7] trust models are developed are based on the infrastructure of provider. Although in those fashions it interferes with dependable Hardware which includes Hardware module (TPM) hardware and software program are exploited however this can't be taken into consideration dependable as TPM is below the bodily manage of the provider. What If the provider is untrusted and no one knows how the trust is said to be established. A maintaining approach is needed to fill this mistrust.

979-8-3503-3531-6/23/$31.00 ©2023 IEEE

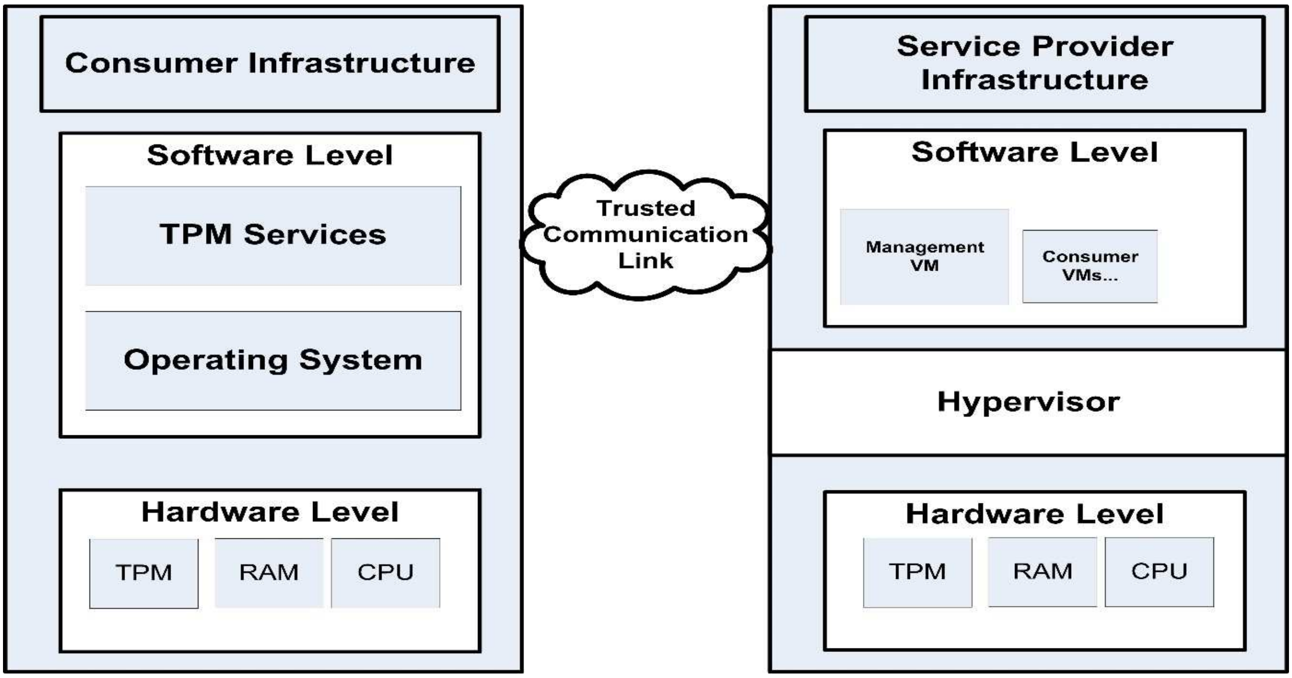

FIGURE 1 GENERALIZED ARCHITECTURE OF DISTRIBUTED TRUSTED CLOUD COMPUTING PLATFORM

It has been assumed withinside the literature that via way of means of permitting the user to manipulate and put in force counter-measures, the user self assurance withinside the cloud may be set up as in [4]. This work is the extension of [8]. Authors proposed a novel technique to increase the trust in the cloud service, the user to take part withinside the safety of cloud-primarily based totally VM. It continues to be allotted among provider and user. According to the patron he makes use of his infrastructure to make counter-security features and test the integrity and confidentiality of the rented VM held via way of means of the provider. The principal aspect of [8] is a tamper-evidence chip referred to as the Trusted Platform Module (TPM). The studies paintings is blanketed withinside the Trusted Computing Group (TCG) rules. This research work extends the contribution made by the authors in [8\ by providing the centralized accessibility to access the hosted VM. The bottleneck of [8] is inaccessibility of hosted VM from different clients. It is in contrast to the nature of the cloud that cloud can be accessed from anywhere. According to the specifications of TCG [9], TPM is immovable hardware chip but, its credentials can be shared with other devices. So, by exploiting the movability of TPM's credentials, we propose a naïve technique to provide client-centric trust mechanism for cloud computing. By doing so, hosted VM can be booted with trusted technology from anywhere and from any device.

According to [10] TPM might be a de facto regulation on all computer systems soon. This prediction supports this research work. In [11], it is reported that in the near past, millions of TPM chip has been embedded in personal computers that are underutilized so far. This model will let the users of cloud computing to fully utilized the TPM chip for the security of cloud environment. Authors have utilized de facto hardware component for enhancing the trust in cloud computing. Figure 1, above depicts the scenario of this proposed model for Cloud. In this illustration, there are two sides of the picture. The right side of the picture shows the cloud computing environment at the provider side. Whereas the left side of the picture shows the cloud computing environment of the consumer side. The consumer has a computer machine through which he/she uses the cloud services and tamper proof hardware chip Trusted Platform Module (TPM) is also attached to it. Trusted computing services are active on the consumer side environment. The right side of the figure above shows the provider environment in which consumer virtual machines are hosted and running. In the Management VM of the provider, side supports the facility of consumer-centric trust mechanism and carries out the communication between the consumer and provider. Each person VM is supported through relied on era of the TCG and digest values calculated through SHA-1 all through boot method are dispatched to the person and person securely saves the values in PCRs of the user TPM.

II. LITERATURE REVIEW

Trust is an vital fragment of cloud computing because cloud user has to store data and perform some sort of computation by outsourcing the third party infrastructure. There are a few approaches thru which agree with in cloud computing may be better consisting of with the aid of using dispensing the obligation of making use of safety countermeasures among the customer and the company. Security duty distribution is also considered as in [6] authors have designed multi-tenancy relied on computing surroundings version (MTCEM) in which the company is chargeable for the safety of host and VMM and customer is chargeable for the safety of VM and the transitive agree with is commenced from OS loader as a substitute from TPM. Based on TCG specifications, TPM is designed for a single OS and one physical platform to work with. Virtualization technique at IaaS layer enables to use TPM in cloud environment. For the virtualization of TPM, IBM applied full specifications of

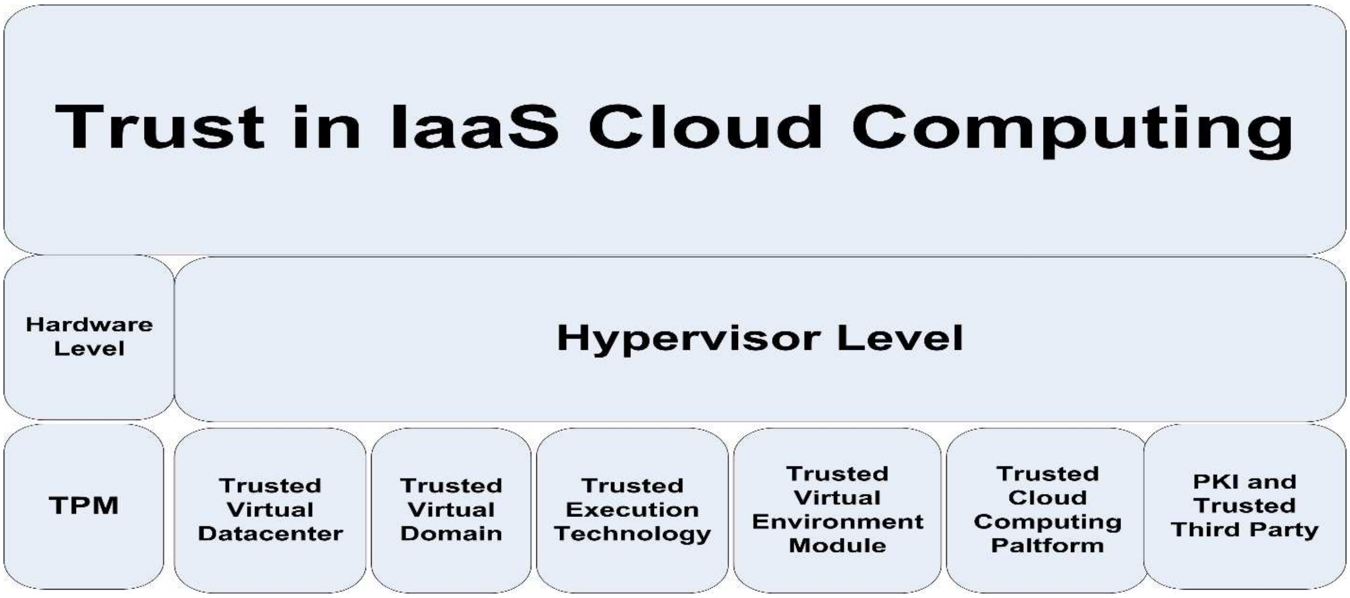
Trust in IaaS Cloud Computing
Hardware Level
Hypervisor Level
TPM
Trusted Virtual Datacenter
Trusted Virtual Domain
Trusted Execution Technology
Trusted Virtual Environment Module
Trusted Cloud Computing Paltform
PKI and Trusted Third Party

FIGURE 2 PROVISION OF TRUST THROUGH TRUSTED COMPUTING TECHNOLOGY FOR DIFFERENT TRUSTED CLOUD COMPUTING PLATFORMS

TCG [12] named vTPM. Authors included vTPM into hypervisor that makes the capabilities availability of TPM to the digital times walking on a hypervisor. vTPM is likewise used in [5] Private Virtual Infrastructure (PVI) to offer the basis of agree with for digital infrastructure. PVI stocks the duty of safety among the company and customer. Trust also can be better with the aid of using letting the customer realize approximately the integrity of the platform as a Trusted Virtual Environment Module (TVEM) [4]. TVEM is a proposed software program module on the digital surroundings of the customer on company's infrastructure that we could the customer confirm the host platform and digital surroundings for agree with worthiness. After verification outcomes are stated to the customer. It also claims to solve shortcomings of vTPM. Trust as a Service is proposed in [13]. Conferring to the Cloud Security Alliance (CSA) provider company have to have much less duty for the safety in IaaS version. In cloud, customer desires reporting and know-how approximately the integrity of rented VM that the configuration isn't always modified with out the consent of customer. [14] provided a tool over which integrity of infrastructure may be measured periodically. It additionally presents faraway attestation cloud computing infrastructure. Trusted Cloud Computing Platform (TCCP) proposed in [7] and applied in [15] the user could use the IaaS offer in closed field for execution of machines (VM) and it additionally lets in the customer to prove the platform and determine either to release machine (VM) or not at the host platform. It desires a Trusted Virtual Machine Monitor and the Trusted Coordinator. TVMM thwarts privileged customers to get admission to the other person machines (VMs) and additionally offer inaccessibility to most of the VMs which can be execute beneath the node. The protocol additionally facilitates to decide whether or not VM is released on a relied on node. IBM provided Trusted Virtual Datacenter (16) includes TPM, vTPM, sHype and cloud control software program for robust isolation and integrity security. Allowing the person to confirm the infrastructure at the provider aspect with the aid of using the usage of Trusted Computing is in general endorsed and considered withinside the literature. Our research work is mainly engrossed on IaaS layer for consumers lease virtual machines on the infrastructure of the provider. The separation in security duty [6]. Any malevolent action from provider drive maltreatment the cloud provider be the probable barricade in the acceptance of cloud computing. Another there ought -to be a cloud computing model does not be subject to upon the structure of the provider for trust in the cloud infrastructure. Trusted computing technology used in cloud computing platforms exist in literature [3], [13], [14]. Most of them have employed physical TPM at cloud provider level [15], [16], [17] and some of them have employed virtual TPM at consumer side [11], [10]. There also exist some trusted platforms that are distributed between consumer and provider [18], [9], [19]. Authors in [14] propose a security framework for the life cycle of the virtual machine and the framework is based on trusted computing. Cloud Security Alliance [20] suggests that the provider must have a lesser duty to secure the cloud computing environment and involve the consumer more in securing the cloud computing platform. In [19] authors present the protocol to measure the integrity of the cloud infrastructure periodically. The protocol enables the consumers to know about the trustworthiness of the cloud computing platform.

III. METHODOLOGY

In this research, we propose a novel technique to access VM in distributed trusted cloud computing that is presented in [8]. This aims to give the pervasive accessibility of the cloud from different types of clients machine. [8] has not facilitated users to access the guest VM from different clients. That's the bottleneck of their research work. Thus, we propose a new model for accessibility of guest VM. According to this research, the cloud user may have computing device having a Trusted Platform Module (TPM) chip attached. It should be noted that [11] millions of these chips are already integrated with all the end user devices. Keeping this fact we propose such a user centric trusted platform. In this paper authors consider the process of TCG's Trusted Boot Process for a VM at provider's infrastructure. According to the method of trusted boot, all the crucial parts of VM such as BIOS, Boot Loader, OS kernel, OS etc. are measured (hashed) during the boot process of VM and measurement values (hash values calculated) are stored in tamper resistant hardware chip. In the proposed architecture TPM resides at the consumer side. After some time upon the consumer restart procured computer (VM), the measured (hashed) values of the machine (VM) i.e (BIOS, Boot Loader, OS kernel, OS etc.) are checked with the measurement values of the previous boot process. If values are not same it can be said that VM components tamper. These values play a significant role in the integrity measurement of VM and in the following discussion.

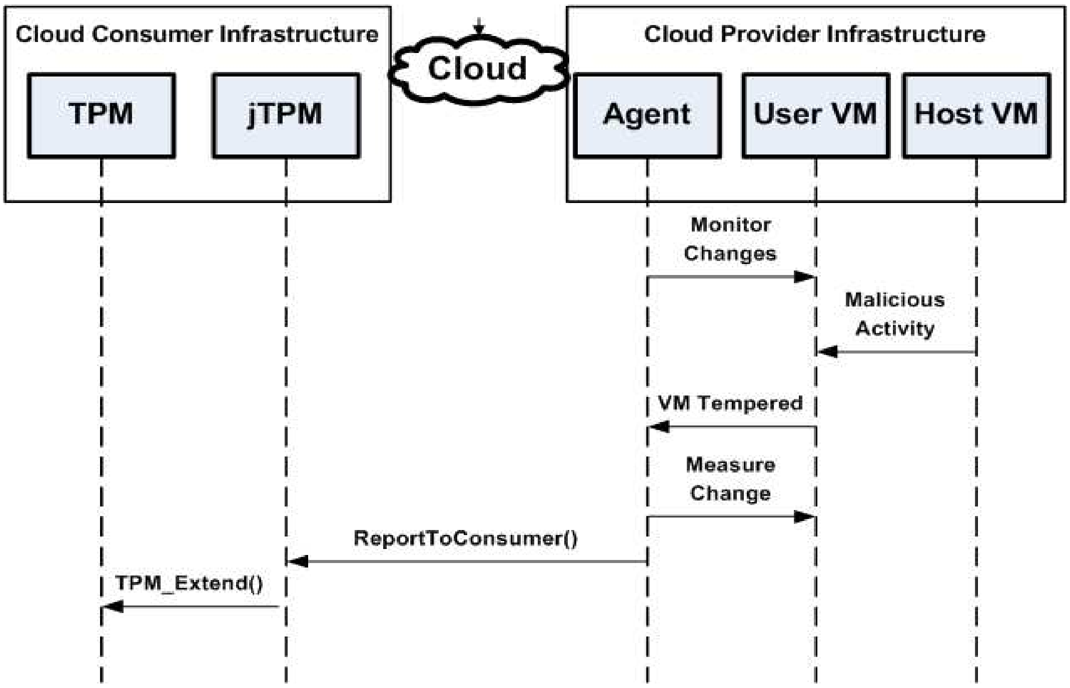

FIGURE 3 VM INTEGRITY CHECKING ALGORITHM IN DISTRIBUTED TRUSTED CLOUD COMPUTING PLATFORM

A. Trsuted Platform Module

Trusted Platform Module TPM [17] is a fiddle resistant hardware fixed on every computer machine. A worldwide consortium is known as the Trusted Computing Group (TCG) (18) is a group of corporations such as HP, Intel, IBM, Microsoft etc. This consortium follows that TPM is de facto standard hardware components in computers. So, it is worth mentioning that availability of TPM chip on every computer is not a big issue. Trusted Platform Module is a fiddle resistant chip or a crypto- coprocessor that is embedded on computing devices. it is based on the specifications of Trusted Computing Group (TCG). It performs cryptographic functions to provide many security services to the end-user of a computer. TPM can generate cryptographic keys and store them as well. Furthermore, cryptographic keys can be used

for device attestation and device integrity checking. For the purpose of device attestation its unique RSA key is used.

B. Trusted Boot Process of a VM

In this paper authors consider the process of TCG's Trusted Boot Process for a machine (VM) at provider's side. In the Trusted Boot, all the crucial parts of VM such as BIOS, Boot Loader, OS kernel, OS etc. are measured (hashed) throughout the boot process of machine and measurement values (hashed values) are stored in TPM. In the proposed architecture TPM resides at the consumer side. Upon the event of the restart of the machine, the measured (hashed) values of machine (BIOS, Boot Loader, OS kernel, OS etc.) are checked with the measurement values of the previous boot process. If values are not same it can be said that VM components are tampered. These values show substantial part in the integrity measurement of VM and in the following discussion.

C. Accessibility of Cloud from Different Devices

As per the criteria of a cloud computing model should be accessible from different devices and locations. Distributed Trusted Cloud Computing that is based on physical TPM makes it unviable because TPM is immoveable chip. To make the cloud accessible from different devices, VM values need to be shared with all those devices from which client wants to access the VM as shown in Figure 3. Integrity Measurement List (IML) contains the measurement values of VM components in encrypted form and these values are stored in PCRs of consumer TPM. These values can be shared with other devices via a synchronization tool. By doing so, the cloud can be accessed from different devices. Communication between cloud consumer and provider is assumed to be safe and trusted as described in (8). After receiving measurement values of guest VM consumer can share these values with other TPM enabled devices as shown in the figure 4 below. It is necessary to mention that the primary device from which guest will be accessed is the only single and simple client machine. This machine can be main and has a responsibility to share the integrity values of guest VM with other consumer devices.

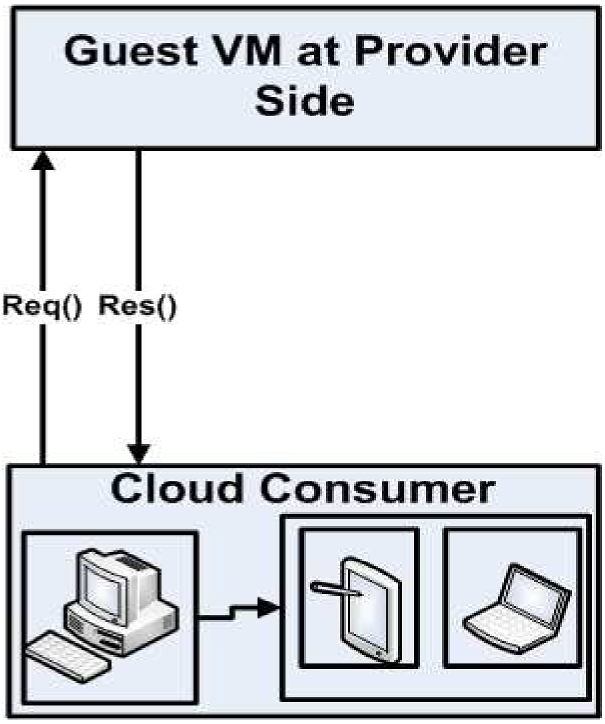

FIGURE 4 CENTRALIZED ACCESSIBILITY OF DISTRIBUTED TRUSTED CLOUD COMPUTING PLATFORM

No.	From and To	Message
1	Cloud Provider->Consumer:	***$\{N, Hash\ (VM_i)\}\ P_s\}AIK_{pub}$***
2	Main Consumer Machine -> other terminals	***$\{\ Hash\ (VM_i)\}\ C_s\}AIK_{pub}$***

Table 1 Algorithm for Centralized Accessibility

keys and symbols used:

- Public Part of Attestation Identity Key (AIK $_{pub}$)
- Session Key (S)
- {} AIK$_{pub}$ Encrypted with AIK$_{pub}$

FUTURE WORK

The future work for the proposed distributed accessibility model for TPM based guest VM is its implementation and an empirical validation of the model in a real scenario. The authors have planned the implementation in Citrix® XenServer® with OpenStack ™ opensource cloud computing platform. It will follow the specifications of the Trusted Computing Group (TCG).

CONCLUSION

Cloud computing is an internet-centric technology for outsourcing IT services such as software, platform, and infrastructure. In this research work accessibility model for the guest VM is proposed. In the proposed model integrity values of guest VM are shared and synchronized with more than one authenticated client devices to access the guest VM from everywhere and anywhere.

REFERENCES

1. Stergiou, Christos, Kostas E. Psannis, Brij B. Gupta, and Yutaka Ishibashi. "Security, privacy & efficiency of sustainable cloud computing for big data & IoT." *Sustainable Computing: Informatics and Systems* 19 (2018): 174-184.

2. Zhang, PeiYun, Yang Kong, and MengChu Zhou. "A domain partition-based trust model for unreliable clouds." *IEEE Transactions on Information Forensics and Security* 13, no. 9 (2018): 2167-2178.

3. Kashif, Ubaidullah Alias, Zulfiqar Ali Memon, Shafaq Siddiqui, Abdul Rasheed Balouch, and Rakhi Batra. "Architectural design of trusted platform for IaaS cloud computing." In *Cloud Security: Concepts, Methodologies, Tools, and Applications*, pp. 393-411. IGI Global, 2019.

4. Krautheim FJ, Phatak DS, Sherman AT. Introducing the trusted virtual environment module: a new

mechanism for rooting trust in cloud computing. Trust and Trustworthy Computing: Springer; 2010. p. 211-27.

5. Montasari, Reza, Alireza Daneshkhah, Hamid Jahankhani, and Amin Hosseinian-Far. "Cloud computing security: Hardware-based attacks and countermeasures." In *Digital Forensic Investigation of Internet of Things (IoT) Devices*, pp. 155-167. Springer, Cham, 2021.

6. Jangjou, Mehrdad, and Mohammad Karim Sohrabi. "A comprehensive survey on security challenges in different network layers in cloud computing." *Archives of Computational Methods in Engineering* (2022): 1-22.

7. Santos N, Gummadi KP, Rodrigues R, editors. Towards trusted cloud computing. Proceedings of the 2009 conference on Hot topics in cloud computing; 2009.

8. Tabrizchi, Hamed, and Marjan Kuchaki Rafsanjani. "A survey on security challenges in cloud computing: issues, threats, and solutions." *The journal of supercomputing* 76, no. 12 (2020): 9493-9532.

9. Sumrall N, Novoa M, editors. Trusted Computing Group (TCG) and the TPM 1.2 Specification. Intel Developer Forum; 2003.

10. Bertholon B, Varrette S, Bouvry P, editors. Certicloud: a novel tpm-based approach to ensure cloud iaas security. Cloud Computing (CLOUD), 2011 IEEE International Conference on; 2011: IEEE.

11. Ibrahim, Fady AM, and Elsayed E. Hemayed. "Trusted cloud computing architectures for infrastructure as a service: Survey and systematic literature review." *Computers & Security* 82 (2019): 196-226.

12. Perez R, Sailer R, van Doorn L, editors. vTPM: virtualizing the trusted platform module. Proc 15th Conf on USENIX Security Symposium; 2006.

13. Noor TH, Sheng QZ. Trust as a service: a framework for trust management in cloud environments. Web Information System Engineering–WISE 2011: Springer; 2011. p. 314-21.

14. Zhang, Peiyun, Mengchu Zhou, and Yang Kong. "A double-blind anonymous evaluation-based trust model in cloud computing environments." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 51, no. 3 (2019): 1805-1816.

15. Landry KN, Babajide J-C, Olufunke SO, Gharaibeh Z, Harold BK. Implementing Trusted Cloud Computing Platform using virtual TPM to achieve Confidentiality and Integrity. Case Study: Amazon EC2. 2011.

16. Berger S, Cáceres R, Pendarakis D, Sailer R, Valdez E, Perez R, et al. TVDc: managing security in the trusted virtual datacenter. ACM SIGOPS Operating Systems Review. 2008;42(1):40-7.

17.http://www.iso.org/iso/catalogue_detail.htm?csnumber=50970.

18. http://www.trustedcomputinggroup.org/. Trusted Computing Group.

19. Kashif, U. A., Memon, Z. A., Balouch, A. R., & Chandio, J. A. (2015, January). Distributed trust protocol for IaaS cloud computing. In Applied Sciences and Technology (IBCAST), 2015 12th International Bhurban Conference on (pp. 275-279). IEEE.

20. Gan, Chenquan, Qingdong Feng, Xulong Zhang, Zufan Zhang, and Qingyi Zhu. "Dynamical propagation model of malware for cloud computing security." *IEEE Access* 8 (2020): 20325-20333.

21. Sun, PanJun. "Security and privacy protection in cloud computing: Discussions and challenges." *Journal of Network and Computer Applications* 160 (2020): 102642.

22. Zhang, Lei, Hu Xiong, Qiong Huang, Jiguo Li, Kim-Kwang Raymond Choo, and Jiangtao Li. "Cryptographic solutions for cloud storage: Challenges and research opportunities." *IEEE Transactions on Services Computing* 15, no. 1 (2019): 567-587.