e-ISSN 2320 –7876 www.ijfans.org
Vol.11, Iss.7, 2022
Research Paper © 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal

Systematic Literature Review Paper Survey Based On Trusted Platform Module

Shikha Singh[1], Dr. Ajay Kumar Bharti[2], Dr. Himanshu Pandey[3], Dr. Durgansh Sharma[4], Dr. N.R.Shanker[5]

IEEE student ,Research Scholar, Computer Science and Engineering[1], Professor,School of Computer Application[2], Assistant Professor, Computer Science and Engineering[3], Associate Professor,School of Business Management[4], Professor,Computer Science and Engineering[5]

Maharishi University of Information and Technology, Lucknow,U.P.,India[1],Babu Banarasi Das University, Lucknow,U.P.,India[2], Lucknow University, Lucknow,U.P.,India[3],Christ University Ghaziabad,U.P.,India[4], Aalim Muhamed Salegh College of Engineering, Chennai,Tamil Naidu,India[5]

ABSTRACT

Trusted Platform Module (TPM) on virtual machine system is a hardware-based root of trust. TPM saves the artefacts necessary to authenticate the computer's platform integrity. The Trusted Computing Group was formed to ensure the Platform's integrity is maintained through the Trusted Platform Module. We perform a thorough review of the literature on cryptographic primitives of trusted computing for infrastructure as a service in this paper. We discuss cloud computing as well as secure computing virtualization.

Key words: Cloud Computing, Virtualization, Trusted Platform Module

INTRODUCTION

Cloud Computing provides remote access to many organizations such as government organizations, financial and health organizations, businesses. Any organization requires the protection of data this trust maintains through the cloud service provider (CSP). (Krautheim et.al.,2010) Cloud Service Providers lower the enormous degree of risk imposed on data centre security. The trustworthiness of a cloud service provider and a cloud consumer is established through data security and privacy. Trusted Computing technologies are responsible for attesting the software platform. Open implementation strategy easily discovers and vulnerabilities, attacks, and other misconfiguration (Kamhoua et.al.,2015). Open implementation cloud infrastructure detected the malicious and legitimate cloud users.

a) Cloud Computing

Cloud computing refers to the offering of on-demand computer services through the internet for a fee based on consumption. Cloud service models have been classified into three types: 1) Software as a service (SaaS) and 2) Platform as a service (PaaS) (Paas) 3) The notion of infrastructure as a service (Iaas). Cloud computing features and benefits Infrastructure as a service and the duties of IaaS providers, as well as IaaS provider facilities (Bhardwaj et.al., 2010). Cloud Storage provides insight into the many types of cloud service models used in cloud computing. The cloud storage address is the location of the cloud storage provider (Rajan et. al.,2013). The preceding technologies of cloud computing and

their relevance. How to tackle the problems and future advancements of these technologies (Ward et. al.,2013).

Two approaches to cloud IaaS deployment The first is an opportunistic technique that allows for the non-intrusive usage of cloud resources, while the second is a virtualization method that provides for on-demand tailored execution environments (Rosales et.al.,2011). The cloud infrastructure as a service concept demonstrates the cheat sheet documentation in the history of information and communication technology (Rumale et.al.,2013). Technical and trust are necessary to examine the cloud forensic exam and offer a review of forensic acquisition tools such as Encase and AccessData Toolkit, which demonstrate the recovery of volatile and non-volatile cloud data. Dykstra et al. (2012)

Cloud service providers provide resource management strategies such as resource allocation, resource mapping, resource provisioning, and resource adaption to improve scalability and service quality (Manvi et.al.,2014). IaaS cloud security is controlled by a cloud trust security assessment methodology that ensures the confidentiality and integrity of the cloud computing system and the cloud service provider. Gonzalez et al.,2015) The Scalable technique is used to analyse the availability of the IaaS cloud. A Markov chain-based technique is used to lessen the complexity of analysis and the time it takes to solve problems. The stochastic reward net is a high-level Petri net paradigm built by Markov chains. Longo et al. (2011)

A survey of cloud providers was conducted, and a taxonomy of Infrastructure as a Service was established, including the resources, business model, deployment, runtime, hardware and performance, and service type (Prodan et. al.,2009). Securing the virtual machine from many forms of assaults in the Infrastructure as a service cloud and rendering intrusion attacks on the virtual machine ineffectual. The Virtual Machine Monitor has a single IP address (Tupakula et.al.2011). Since of third-party services, cloud computing poses a danger because it is difficult to ensure data security and privacy. (Hashizume et al.,2013). The Trusted Computing Environment adds secrecy, integrity, and authentication to cloud computing security (Shen et.al.,2010)

b) Virtualization

The differences and similarities between the virtualization of server and cloud computing models will help digital library managers (Cervone,2010). The role of hardware and software virtualization in cloud computing applications and its benefits.(Jain et.al.,2016; Khajehei et. al.2014).Different aspects of cloud security virtualization and identified the security requirement of virtualization infrastructure cloud, attacks, security solution(Kazim et.al.,2013; Luo et.al.2011).

Virtualization improves cloud computing security by securing the virtual machine and cloud infrastructure. Advanced Cloud Protection System (ACPS), a revolutionary technique, boosted the security of cloud resources while efficiently monitoring the virtual machine and cloud user. ACPS implemented the open-source solution: Eucalyptus and Open ECP. The prototype of ACPS is tested effectiveness testing against attacks and performance evaluation of different types of workload (Lombardi et.al., 2011).Hardware trust of virtualization and isolation initial start from tenants. Virtualization technique to solve the different challenges of software and hardware layer.(Bouali,et.al.,2016).

 © 2012 IJFANS. All Rights Reserved,

c) Trusted Platform Module

Purpose of providing hardware-based safety features, a Trusted Platform Module is being proposed. The Trusted Platform Module chip is a secure crypto-processor that helps with cryptographic key storage, creation, and limiting. (Bourguiba et. al,2013).

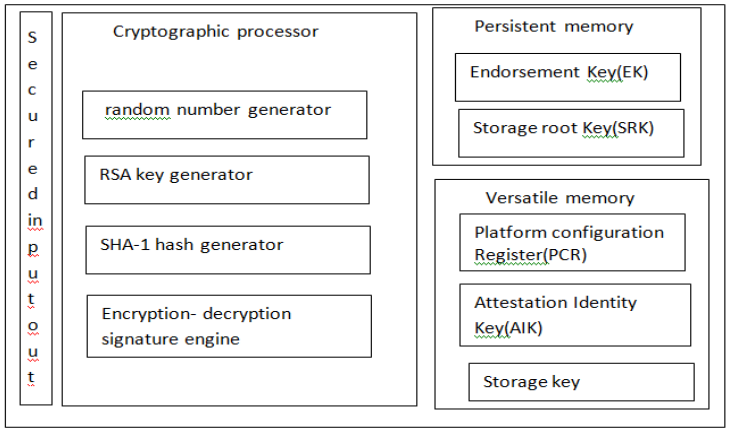

Figure1. Trusted Platform Module Component

II. Systematic Literature review on Trusted Platform Module

Dynamic Website Content Monitoring and Alerting for Defacement Using Trusted Platform Module in this study proposed that software system uses operating system kernel file system monitor to detect changes and integrate with hardware system known as Trusted platform Module for dynamic web site content (Viswanathan et.al. 2016).

This authors recommended for a comparative research based on trusted computing scheme integration of TPM in IoT computing execute a cryptographic operation and hardware-based security to counter cyber security challenges (Faisal et.al. 2020).

Crowd Quality Control Using Remote Attestation on Behavioural Traces This study recommended, based on Trusted Platform Module, that Trusted Platform Module recorded and stored behavioural traces in storage measurement log (SML) and platform configuration register (PCR). The PCR and SML evidence value provided to TPM signature with the crowdsourcing platform. A remote attestation protocol is used to construct the SML hash process (Fu et. al.,2021).

TPM in Cyber-Physical Systems: On the Interference Between Dependability and Security concentrated on determining the equilibrium state between security and dependability interferences on Trusted Platform Module services in this study (Hoeller et. al.,2018).

A Trusted Platform Cloud Certificate Authority Architecture for Virtual Machines The Trusted Module Platform operation is maintained by Modul in this article, which focuses on certificate authority. Virtual machines are intended to be secure. The measurement algorithm is utilised for the virtual machine's user authentication process (Yu et.al.,2015).

Protecting Agents from Malicious Hosts Using Trusted Platform Modules (TPM) was the topic of this research, which argued for a unique way to protecting infrastructure services

for Trusted Platform Module processing services. They suggest moving the protocol and improving the Java Agent Development Framework in their proposed system (Md Ali Shaik,2018).

ICITPM: In this article, we focused on authentication and the integrity of source code and binary files used in Trusted Platform Module. (Muniz et al.,2020).

On the Raspberry Pi, we are simulating the trusted platform module 2.0. 2 in this Trusted Computing Group recommended Trusted Platform Module through IBM implementation software Trusted Platform Module (STPM) version install on RPi2 and assess performance with TPM Command (Cheng et. al.,2020).

This study focused on TPM extension Scheme (xTSeH) suggested with TPM installed smart embedded devices (TSED). Trusted base kernel module created a shadow TPM type of non-TPM protected SED (N-TSED) that was implemented using the Raspberry Pi protocol (Lu et.al.,2020).

Integrating Trusted Platform Modules in Power Electronics focuses on integrating TPM in a system implemented Advanced Reduction Instruction Set Machine (ARM) processor for power electronics security (Khan et.al.,2020).

Proactive Proper Security Management with a Focus on Peer Service Notification ARMing the TPM We focused on proactive integrity reporting and monitoring of the TPM via the peer system in this essay. (Maybaum et.at.,2015).

A TA for VM on Cloud Servers with TPM and CA focuses on the trust built using the Trusted Platform Module (TPM) and the Certificate Authority (CA) of TPM operation for virtual machine maintenance and security. For the VM authentication mechanism, a measurement algorithm is employed (Yu et.al.,2017).

A More Secure Scheme for Virtual TPMs This article focused on security enhanced approach using asymmetric encryption algorithm for virtual Trusted Platform Module security based on Kernel Virtual Machine (KVM) in this paper (Shi et.al.,2015).

Cryptographic Considerations for SCADA and Automation Systems Using TPA advocated that different perspectives of a security issue for automation/supervisory control and data acquisition (SCADA) with Modbus TCP protocol based on the function of integrated Trusted Platform Modules be advocated in this paper (Tidera et. al.,2019).

This article focused on HMAC authorization security protocol examined with digital rights management in TPA 2.0 hash-based message Verification code authorization under management scenario digital rights (Yu et.al.,2016).

Handling compromised components in an IaaS cloud installation is the topic of this article, which focuses on the Openstack Infrastructure as a service. In the cloud environment, incident handling is required for function adjustment (Taheri Monfared et. al.,2012). The study Software Emulation of Quantum Resistant Trusted Platform Modules focused on three Post Quantum (PQ) techniques utilised on non-quantum Resistant TPMs via software emulation (Fiothais et.al.2020). Using Hardware-Based Virtualization to Improve Trusted Platform Modules This paper's techniques argued for numerous virtual machines to preserve their hardware TPM. The TPM scheduling and management instructions are monitored by the virtual machine(Stumpf et. al.,2008).

 © 2012 IJFANS. All Rights Reserved,

This study focused on trusted-Flex utilised for Trusted platform Module for security services such as confidentiality, integrity, and authenticity based on RSA public key and XTEA symmetric key cryptography of wireless Sensor network (Hu et.al.,2010).

This paper advocated that TVEM helps to solve the virtual environment of the service provider Trusted Platform Module virtualization technique to assist the cryptography algorithm, application programme interface, and configurable modular architecture in Introducing the Trusted Virtual Environment Module: A New Mechanism for Rooting Trust in Cloud Computing(Krautheim et.al.,2010).

In this work, Trusted Wireless Sensor Node Platform recommended for Trusted Platform Module with 32-bit ARM 11 CPU for wireless sensor node platform security implementation (Yussoff et.al.,2010).

This research focused on simulation toolset estimation of Trusted Platform Module Services as Scalable Architectural Support for Trusted Software. TPM-based performance optimization improves in two ways. The initial step is to take use of the numerous TPM, followed by sorting the request and decreasing the queue. (Schmitz et. al.,2011) This study focused on the ARM trusted area utilised in TEE of tablets and smartphones in Trusted Execution Environments on Mobile Devices. TEEs environment is provided via on-board credentials and mobile phones. The Trusted Platform Module quickly discovers hardware security problems (Ekberg et.al.,2013).

This article focuses on the Bastion hardware-software architecture, which improved the microprocessor hardware and hypervisor software. Trusted Platform Module is a cutting-edge security chip in today's market. They reflect the OpenSPARC platform's implementation (Champagne et.al.,2010). This study focused on implementing the Needham-Schroeder public-key protocol for cloud architecture's trusted Platform Modules in a new cloud architecture with virtual Trusted Platform Modules (Liu et al.,2012).

Trusted Platform-as-a-Service: A Foundation for Trustworthy Cloud-Hosted Applications is a paper that focuses on how a trusted third-party cloud provider manages the host application's architecture and platform. Python/Django web framework supports cloud provider's trusted Platform as a service (Brown et.al.,2013). In this study focuses on crucial objects of informatics calculations of any industry or organisation dependent on hardware platform module with Trusted Certification (Vorobiev et.al.,2017). This study, Design and Implementation of Mobile Trusted Module for Trusted Mobile Computing, focused on MTMs used for mobile devices, similar to TPMs used for PCs. MTM design based on a spatially optimised architecture with 400 logic gates and a power consumption of 10mA for trusted computing (Kim et.al.,2010).

Network protocol of different controller is the topic of this study by allowing users to assess the safety of accessible interfaces, NFC contributes to the Trusted platform module architecture Platform Module with Trusted Certification In this article, a survey argued for the security of TPM design and functioning. TPM resolves data-related bootstrap security and authorisation security issues (Ezirim et.al., 2012).

This study, Towards a Virtual Trusted Platform, pushed for trusted computing and hardware-assisted strong virtual platforms for software security. Through Intel Trusted

 © 2012 IJFANS. All Rights Reserved,

Execution Technology, Trusted Platform Module and hardware-assisted virtualization boots manipulation are possible (Pirker et.al.,2010). This study, Cloud Computing System Based on Trusted Computing Platform, focused on the security requirements of the cloud computing environment. Based on a trusted platform module, a prototype provides a mix of cloud computing and Trusted platform support services (Shen et.al.,2010). In this work, we will expand the SSL/TLS protocol on TPM to overcome security issues with the SSL/TLS protocol based on TPM (Yu et.al.,2010).

The article Reconfigurable Dynamic TPM for Control Flow Checking focuses on the dynamic TPM architecture in FPGA that conducts control flow checking (Das et.al.,2014).Using a Trusted Platform Module to Mitigate Botnet Attacks is a study that focuses on botnets, which are rising dangers to online transactions. A trusted platform module framework reduces the danger of botnet attacks on online banking apps (Sidheeq et.al.,2010). A hijacker's guide to the trusted platform module's communication interfaces in this study focused on the trusted platform module and its interfaces to manipulate communication buses and embedded systems (Winter et.al.,2013).

TPM for Smart Cards is a paper that focuses on near spectrum data transmission smartphone services and provides multiplications smartcard architecture cross-device security via reliable executable and consumer tamper-resistant gadget via trusted execution environment and user-centric tamper-resistant device. Between the application and the service provider, a TPM for portable systems (smartcards) builds trust (Akram et. al.,2014).
A reliable Real Field communication platform module.The use of Dedicated short range communication (NFC) to the secure(Hutter et.al.,2010) this study argued for a new cloud architecture of virtual trusted platform module to increase the usability and security of cloud architecture of virtual TPM functionality by using the Needham Schroeder public-key protocol (Liu et al.,2012).
Using TPM to Secure Business Communication (SBC) in Vehicular Ad hoc Network (VANET) in this focused on trusted platform module demonstrate the importance of SBC between the user and business parties in Vehicular Ad hoc Network (VANET) (Sumra et. al.,2016).Trusted Wireless Sensor Node Platform in this paper focused on trusted platform module technologies initiatives embedded security utilizing 32-bit ARM11 processor security enhance sensor node platform(Yussoff et. al.,2010).

This systematic literature survey is based on three phases first one formulating the search, the second searching, third search result. The first phase of the systematic literature review is designing the search so that the author may select the paper related to the issue. In the second step of systematic literature searches, we acquire a list of 100 publications on the relevant topic from 2010 to 2021. Using this method, we receive a list of 56 papers from which to choose. The third phase thorough literature search reveals that various attackers cannot simply remove the Trusted Platform Module's certificate authority.

 © 2012 IJFANS. All Rights Reserved,

Total no. of Paper Year wise													
Year	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Total
IEEE	6	3		1	2	3	1	1	2		3		22
Springer	1		1	1		1	1	1			1		7
Elsevier		1	1	2	1								5
Wiley							1						1
Others	7	1	2	4	1		1			1	2	2	21
													56

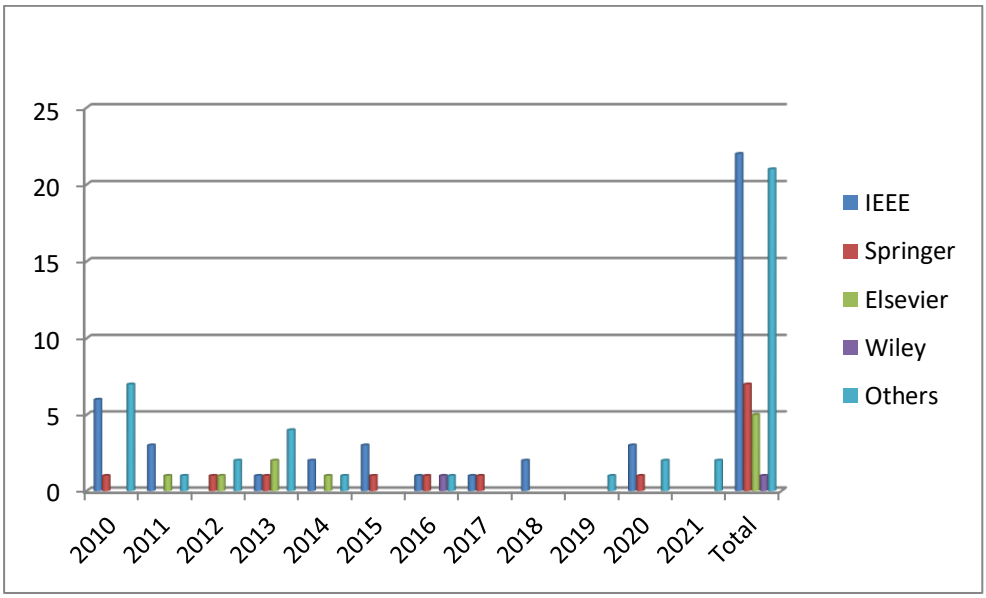

Figure2. Papers Published Journal wise every year from 2010 to 2021

Figure3. Total number of paper year wise

III. Conclusion

TPM adds hardware-based security benefits to the data centre of a cloud service provider.TPM install on hardware i.e. computer remarkably improved security benefits. We analyze the systematic Literature survey report that all the papers depict TPM chip cannot easily accessible from any attackers to reach hardware.

REFERENCES

1) Krautheim, F. J. (2010). *Building trust into utility cloud computing*. University of Maryland, Baltimore County.
2) Kamhoua, C. A., Ruan, A., Martin, A., & Kwiat, K. A. (2015, December). On the feasibility of an and open-implementation cloud infrastructure: A game-theoretic analysis. In *2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC)* (pp. 217-226). IEEE.
3) Tupakula, U., & Varadharajan, V. (2011, December). Tvdsec: Trusted virtual domain security. In *2011 Fourth IEEE International Conference on Utility and Cloud Computing* (pp. 57-64). IEEE.
4) Jaiswal, P. R., & Rohankar, A. W. (2014). Infrastructure as a service: security issues in cloud computing. *International Journal of Computer Science and Mobile Computing*, *3*(3), 707-711.
5) Bhardwaj, S., Jain, L., & Jain, S. (2010). Cloud computing: A study of infrastructure as a service (IAAS). *International Journal of engineering and information Technology*, *2*(1), 60-63.
6) Rajan, A. P. (2013). Evolution of cloud storage as cloud computing infrastructure service. *arXiv preprint arXiv:1308.1303*.
7) Ward, J. S., & Barker, A. (2013). A cloud computing survey: Developments and future trends in infrastructure as a service computing. *arXiv preprint arXiv:1306.1394*.
8) Rosales, E., Castro, H., & Villamizar, M. (2011). Unacloud: Opportunistic cloud computing infrastructure as a service. *Cloud Computing*, 187-194.
9) Rumale, A. S., & Chaudhari, D. N. (2013). Cloud computing: Infrastructure as a service. *International Journal of Inventive Engineering and Sciences*, *1*(3), 1-7.
10) Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation*, *9*, S90-S98.
11) Manvi, S. S., & Shyam, G. K. (2014). Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey. *Journal of network and computer applications*, *41*, 424-440.
12) Gonzales, D., Kaplan, J. M., Saltzman, E., Winkelman, Z., & Woods, D. (2015). Cloud-trust—A security assessment model for infrastructure as a service (IaaS) clouds. *IEEE Transactions on Cloud Computing*, *5*(3), 523-536.
13) Longo, F., Ghosh, R., Naik, V. K., & Trivedi, K. S. (2011, June). A scalable availability model for Infrastructure-as-a-service cloud. In *2011 IEEE/IFIP 41st International Conference on Dependable Systems & Networks (DSN)* (pp. 335-346). IEEE.
14) Prodan, R., & Ostermann, S. (2009, October). A survey and taxonomy of infrastructure as a service and web hosting cloud providers. In *2009 10th IEEE/ACM International Conference on Grid Computing* (pp. 17-25). IEEE.
15) Repschlaeger, J., Wind, S., Zarnekow, R., & Turowski, K. (2012, January). A reference guide to cloud computing dimensions: infrastructure as a service classification framework. In *2012 45th Hawaii International Conference on System Sciences* (pp. 2178-2188). IEEE.
16) Tupakula, U., Varadharajan, V., & Akku, N. (2011, December). Intrusion detection techniques for infrastructure as a service cloud. In *2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing* (pp. 744-751). IEEE.
17) Wallom, D. C., Turilli, M., Drescher, M., Scardaci, D., & Newhouse, S. (2015, August). Federating infrastructure as a service cloud computing systems to create a uniform e-

infrastructure for research. In *2015 IEEE 11th International Conference on e-Science* (pp. 155-164). IEEE.

18) Xia, Y., Zhou, M., Luo, X., Zhu, Q., Li, J., & Huang, Y. (2013). Stochastic modeling and quality evaluation of infrastructure-as-a-service clouds. *IEEE Transactions on Automation Science and Engineering*, *12*(1), 162-170.

19) Srivastava, K., & Kumar, A. (2011). A new approach of a cloud: Computing infrastructure on demand. *Trends in Information Management*, *7*(2).

20) Kumar, R., Jain, K., Maharwal, H., Jain, N., & Dadhich, A. (2014). Apache Cloudstack: Open-source infrastructure as a service cloud computing platform. *Proceedings of the International Journal of advancement in Engineering Technology, Management and Applied Science*, *111*, 116.

21) Rana, P., Gupta, P. K., & Siddavatam, R. (2014). The combined and improved framework of infrastructure as a service and platform as a service in cloud computing. In *Proceedings of the Second International Conference on Soft Computing for Problem Solving (SocProS 2012), December 28-30, 2012* (pp. 831-839). Springer, New Delhi.

22) Arora, P., Wadhawan, R. C., & Ahuja, E. S. P. (2012). Cloud computing security issues in infrastructure as a service. *International journal of advanced research in computer science and software engineering*, *2*(1).

23) Cervone, H. F. (2010). An overview of virtual and cloud computing. *OCLC Systems & Services: International digital library perspectives*.

24) Jain, N., & Choudhary, S. (2016, March). Overview of virtualization in cloud computing. In *2016 Symposium on Colossal Data Analysis and Networking (CDAN)* (pp. 1-4). IEEE.

25) Bourguiba, M., Haddadou, K., El Korbi, I., & Pujolle, G. (2013). Improving network I/O virtualization for cloud computing. *IEEE Transactions on Parallel and Distributed Systems*, *25*(3), 673-681.

26) Kazim, M., Masood, R., Shibli, M. A., & Abbasi, A. G. (2013, September). Security aspects of virtualization in cloud computing. In *IFIP International Conference on Computer Information Systems and Industrial Management* (pp. 229-240). Springer, Berlin, Heidelberg.

27) Lombardi, F., & Di Pietro, R. (2011). Secure virtualization for cloud computing. *Journal of network and computer applications*, *34*(4), 1113-1122.

28) Luo, S., Lin, Z., Chen, X., Yang, Z., & Chen, J. (2011, December). Virtualization security for cloud computing service. In *2011 International Conference on Cloud and Service Computing* (pp. 174-179). IEEE.

29) Khajehei, K. (2014). Role of virtualization in cloud computing. *International Journal of Advanced Research in Computer Science and Management Studies*, *2*(4).

30) Malhotra, L., Agarwal, D., & Jaiswal, A. (2014). Virtualization in cloud computing. *J. Inform. Tech. Softw. Eng*, *4*(2), 1-3.

31) Rankothge, W., Ma, J., Le, F., Russo, A., & Lobo, J. (2015, May). Towards making network function virtualization a cloud computing service. In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)* (pp. 89-97). IEEE.

32) Bourguiba, M., Haddadou, K., El Korbi, I., & Pujolle, G. (2013). Improving network I/O virtualization for cloud computing. *IEEE Transactions on Parallel and Distributed Systems*, *25*(3), 673-681.

33) https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/trusted-platform-module-top-node

34) Viswanathan, N., & Mishra, A. (2016). Dynamic monitoring of website content and alerting defacement using a trusted platform module. In *Emerging research in computing, information, communication, applications* (pp. 117-126). Springer, Singapore.

35) Faisal, M., Ali, I., Khan, M. S., Kim, S. M., & Kim, J. (2020). Establishment of Trust in the Internet of Things by Integrating Trusted Platform Module: To Counter Cybersecurity Challenges. *Complexity*, *2020*.

36) Fu, D., & Liu, Y. (2021). Remote Attestation on Behavioral Traces for Crowd Quality Control Based on Trusted Platform Module. *Security and Communication Networks*, *2021*.

37) Hoeller, A., & Toegl, R. (2018, April). Trusted platform modules in cyber-physical systems: On the interference between security and dependability. In *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 136-144). IEEE.
38) Yu, Z., Wang, Q., Zhang, W., & Dai, H. (2015, August). A cloud certificate authority architecture for virtual machines with a trusted platform module. In *2015 IEEE 17th International Conference on High-Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems* (pp. 1377-1380). IEEE.
39) Shaik, M. A. (2018, April). Protecting agents from malicious hosts using trusted platform modules (TPM). In *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)* (pp. 559-564). IEEE.
40) Muñoz, A., Farao, A., Correia, J. R. C., & Xenakis, C. (2020, September). ICITPM: integrity validation of software in iterative continuous integration through the use of Trusted Platform Module (TPM). In *European Symposium on Research in Computer Security* (pp. 147-165). Springer, Cham.
41) Cheng, J. L. (2020). Emulating Trusted Platform Module 2.0 on Raspberry Pi 2. *International Journal of Security, Privacy and Trust Management (IJSPTM) Vol*, *9*.
42) Lu, D., Han, R., Shen, Y., Dong, X., Ma, J., Du, X., & Guizani, M. (2020). xTSeH: A trusted platform module sharing scheme towards smart IoT-eHealth devices. *IEEE Journal on Selected Areas in Communications*, *39*(2), 370-383.
43) Khan, A., Blair, N., Farnell, C., & Mantooth, H. A. (2020, October). Integrating Trusted Platform Modules in Power Electronics. In *2020 IEEE CyberPELS (CyberPELS)* (pp. 1-5). IEEE.
44) Maybaum, M., & Toelle, J. (2015, October). ARMing the Trusted Platform Module pro-active system integrity monitoring focussing on peer system notification. In *MILCOM 2015-2015 IEEE Military Communications Conference* (pp. 1584-1589). IEEE.
45) Ruchkin, V., Fulin, V., Romanchuk, V., Koryachko, A., & Ruchkina, E. (2020, May). Personal Trusted Platform Module for the Multi-Core System of 5G Security and Privacy. In *2020 ELEKTRO* (pp. 1-4). IEEE.
46) Yu, Z., Zhang, W., & Dai, H. (2017). A trusted architecture for virtual machines on cloud servers with a trusted platform module and certificate authority. *Journal of Signal Processing Systems*, *86*(2-3), 327-336.
47) Shi, Y., Zhao, B., Yu, Z., & Zhang, H. (2015). A security-improved scheme for virtual TPM based on KVM. *Wuhan University Journal of Natural Sciences*, *20*(6), 505-511.
48) Tidrea, A., Korodi, A., & Silea, I. (2019). Cryptographic considerations for automation and SCADA systems using trusted platform modules. *Sensors*, *19*(19), 4191.
49) Yu, F., Zhang, H., Zhao, B., Wang, J., Zhang, L., Yan, F., & Chen, Z. (2016). A formal analysis of Trusted Platform Module 2.0 hash-based message authentication code authorization under digital rights management scenario. *Security and Communication Networks*, *9*(15), 2802-2815.
50) Han, S., Shin, W., Park, J. H., & Kim, H. (2018). A bad dream: Subverting a trusted platform module while you are sleeping. In *27th {USENIX} Security Symposium ({USENIX} Security 18)* (pp. 1229-1246).
51) TaheriMonfared, A., & Jaatun, M. G. (2012). Handling compromised components in an IaaS cloud installation. *Journal of Cloud Computing: Advances, Systems, and Applications*, *1*(1), 1-21.
52) Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of internet services and applications*, *4*(1), 1-13.
53) Fiolhais, L., Martins, P., & Sousa, L. (2020). Software Emulation of Quantum Resistant Trusted Platform Modules. In *ICETE (2)* (pp. 477-484).
54) Stumpf, F., & Eckert, C. (2008, August). Enhancing trusted platform modules with hardware-based virtualization techniques. In *2008 Second International Conference on Emerging Security Information, Systems and Technologies* (pp. 1-9). IEEE.
55) Bouali, L., Abd-Elrahman, E., Afifi, H., Bouzefrane, S., & Daoui, M. (2016, June). Virtualization techniques: Challenges and opportunities. In *International Conference on Mobile, Secure, and Programmable Networking* (pp. 49-62). Springer, Cham.

56) Krautheim, F. J., Phatak, D. S., & Sherman, A. T. (2010, June). Introducing the trusted virtual environment module: a new mechanism for rooting trust in cloud computing. In *International Conference on Trust and Trustworthy Computing* (pp. 211-227). Springer, Berlin, Heidelberg.
57) Hu, W., Tan, H., Corke, P., Shih, W. C., & Jha, S. (2010). Toward trusted wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, *7*(1), 1-25.
58) Yussoff, Y. M., & Hashim, H. (2010). Trusted wireless sensor node platform. *memory*, *3*, 6.
59) Wagan, A. A., Mughal, B. M., & Hasbullah, H. (2010, February). VANET security framework for trusted grouping using TPM hardware. In *2010 Second International Conference on Communication Software and Networks* (pp. 309-312). IEEE.
60) Shen, Z., & Tong, Q. (2010, July). The security of cloud computing systems is enabled by trusted computing technology. In *2010 2nd International Conference on Signal Processing Systems* (Vol. 2, pp. V2-11). IEEE.
61) Champagne, D., & Lee, R. B. (2010, January). Scalable architectural support for trusted software. In *HPCA-16 2010 The Sixteenth International Symposium on High-Performance Computer Architecture* (pp. 1-12). IEEE.
62) Schmitz, J., Loew, J., Elwell, J., Ponomarev, D., & Abu-Ghazaleh, N. (2011, June). TPM-SIM: A framework for performance evaluation of Trusted Platform Modules. In *2011 48th ACM/EDAC/IEEE Design Automation Conference (DAC)* (pp. 236-241). IEEE.
63) Ekberg, J. E., Kostiainen, K., & Asokan, N. (2013, November). Trusted execution environments on mobile devices. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (pp. 1497-1498).
64) Liu, D., Lee, J., Jang, J., Nepal, S., & Zic, J. (2012). A new cloud architecture of virtual trusted platform modules. *IEICE transactions on information and systems*, *95*(6), 1577-1589.
65) Brown, A., & Chase, J. S. (2011, October). Trusted platform-as-a-service: a foundation for trustworthy cloud-hosted applications. In *Proceedings of the 3rd ACM workshop on Cloud computing security workshop* (pp. 15-20).
66) Vorobiev, E. G., Petrenko, S. A., Kovaleva, I. V., & Abrosimov, I. K. (2017, May). Organization of the entrusted calculations in crucial objects of informatization under uncertainty. In *2017 XX IEEE International Conference on Soft Computing and Measurements (SCM)* (pp. 299-300). IEEE.
67) Kim, M., Ju, H., Kim, Y., Park, J., & Park, Y. (2010). Design and implementation of mobile trusted module for trusted mobile computing. *IEEE Transactions on Consumer Electronics*, *56*(1), 134-140.
68) Ezirim, K., Khoo, W., Koumantaris, G., Law, R., & Perera, I. M. (2012). Trusted Platform Module–A Survey. *The Graduate Center of The City University of New York*, 11.
69) Pirker, M., & Toegl, R. (2010). Towards a Virtual Trusted Platform. *J. Univers. Comput. Sci.*, *16*(4), 531-542.
70) Shen, Z., Li, L., Yan, F., & Wu, X. (2010, May). Cloud computing system based on the trusted computing platform. In *2010 International Conference on Intelligent Computation Technology and Automation* (Vol. 1, pp. 942-945). IEEE.
71) Yu, Y., Sun, H., & Kong, Y. (2010, October). Expand the SSL/TLS protocol on the trusted platform module. In *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)* (Vol. 11, pp. V11-48). IEEE.
72) Das, S., Zhang, W., & Liu, Y. (2014, July). Reconfigurable dynamic trusted platform module for control flow checking. In *2014 IEEE Computer Society Annual Symposium on VLSI* (pp. 166-171). IEEE.
73) Sidheeq, M., Dehghantanha, A., & Kananparan, G. (2010, December). Utilizing a trusted platform module to mitigate botnet attacks. In *2010 International Conference on Computer Applications and Industrial Electronics* (pp. 245-249). IEEE.
74) Hutter, M., & Toegl, R. (2010, August). A trusted platform module for near-field communication. In *2010 Fifth International Conference on Systems and Networks Communications* (pp. 136-141). IEEE.

75) Winter, J., & Dietrich, K. (2013). A hijacker's guide to communication interfaces of the trusted platform module. *Computers & Mathematics with Applications*, *65*(5), 748-761.
76) Kursawe, K., Schellekens, D., & Preneel, B. (2005, September). Analyzing trusted platform communication. In *ECRYPT Workshop, CRASH-CRyptographic Advances in Secure Hardware* (p. 8).
77) Akram, R. N., Markantonakis, K., & Mayes, K. (2014, March). Trusted platform module for smart cards. In *2014 6th International Conference on New Technologies, Mobility and Security (NTMS)* (pp. 1-5). IEEE.
78) Han, S., Shin, W., Park, J. H., & Kim, H. (2018). A bad dream: Subverting a trusted platform module while you are sleeping. In *27th {USENIX} Security Symposium ({USENIX} Security 18)* (pp. 1229-1246).
79) Liu, D., Lee, J., Jang, J., Nepal, S., & Zic, J. (2012). A new cloud architecture of virtual trusted platform modules. *IEICE transactions on information and systems*, *95*(6), 1577-1589.
80) Khmelevsky, Y., & Voytenko, V. (2010, May). Cloud computing infrastructure prototype for university education and research. In *Proceedings of the 15th Western Canadian Conference on Computing Education* (pp. 1-5).
81) Dong, B., Zheng, Q., Yang, J., Li, H., & Qiao, M. (2009, July). An e-learning ecosystem based on cloud computing infrastructure. In *2009 Ninth IEEE International Conference on Advanced Learning Technologies* (pp. 125-127). IEEE.
82) Rajan, A. P. (2013). Evolution of cloud storage as cloud computing infrastructure service. *arXiv preprint arXiv:1308.1303*.
83) Yildiz, M., Abawajy, J., Ercan, T., & Bernoth, A. (2009, December). A layered security approach for cloud computing infrastructure. In *2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks* (pp. 763-767). IEEE.
84) Dikaiakos, M. D., Katsaros, D., Mehra, P., Pallis, G., & Vakali, A. (2009). Cloud computing: Distributed internet computing for IT and scientific research. *IEEE Internet computing*, *13*(5), 10-13.
85) Goyal, T., Singh, A., & Agrawal, A. (2012). Cloudsim: simulator for cloud computing infrastructure and modeling. *Procedia Engineering*, *38*, 3566-3572.
86) Kang, C., & Wei-Min, Z. (2009). Cloud computing: system instances and current research.
87) Dougherty, B., White, J., & Schmidt, D. C. (2012). Model-driven auto-scaling of green cloud computing infrastructure. *Future Generation Computer Systems*, *28*(2), 371-378.
88) Ukil, A., Jana, D., & De Sarkar, A. (2013). A security framework in cloud computing infrastructure. *International Journal of Network Security & Its Applications*, *5*(5), 11.
89) Achemlal, M., Gharout, S., & Gaber, C. (2011, May). Trusted platform module as an enabler for security in cloud computing. In *2011 Conference on Network and Information Systems Security* (pp. 1-6). IEEE.
90) Shen, Z., Li, L., Yan, F., & Wu, X. (2010, May). Cloud computing system based on trusted computing platform. In *2010 International Conference on Intelligent Computation Technology and Automation* (Vol. 1, pp. 942-945). IEEE.
91) Kashif, U. A., Memon, Z. A., Siddiqui, S., Balouch, A. R., & Batra, R. (2019). Architectural design of trusted platform for IaaS cloud computing. In *Cloud Security: Concepts, Methodologies, Tools, and Applications* (pp. 393-411). IGI Global.
92) Santos, N., Gummadi, K. P., & Rodrigues, R. (2009). Towards Trusted Cloud Computing. *HotCloud*, *9*(9), 3.
93) Brohi, S. N., Bamiah, M. A., Brohi, M. N., & Kamran, R. (2012, December). Identifying and analyzing security threats to virtualized cloud computing infrastructures. In *2012 International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM)* (pp. 151-155). IEEE.
94) Krautheim, F. J. (2009). Private Virtual Infrastructure for Cloud Computing. *HotCloud*, *9*, 1-5.
95) Sule, M. J., Li, M., Taylor, G. A., & Furber, S. (2015, September). Deploying trusted cloud computing for data intensive power system applications. In *2015 50th International Universities Power Engineering Conference (UPEC)* (pp. 1-5). IEEE.

96) Patidar, K., Gupta, R., Singh, G., Jain, M., & Shrivastava, P. (2012). Integrating the trusted computing platform into the security of cloud computing system. *International Journal of Advanced Research in Computer Science and Software Engineering*, *2*(2).

97) Han-Zhang, W., & Liu-Sheng, H. (2010, October). An improved trusted cloud computing platform model based on DAA and privacy CA scheme. In *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)* (Vol. 13, pp. V13-33). IEEE.

98) Padma, E., & Rajalakshmi, S. (2017). Trusted Attestation System for Cloud Computing Environment Using Trusted Platform Module. *Internet of Things and Cloud Computing*, *5*(3), 38.

99) Fera, M. A., & Priya, M. S. (2016). A Survey on Trusted Platform Module for Data Remanence in Cloud. In *Proceedings of the International Conference on Soft Computing Systems* (pp. 689-695). Springer, New Delhi.

100) Bouzefrane, S. (2014, August). Trusted platforms to secure mobile cloud computing. In *2014 IEEE Intl Conf on High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl Conf on Embedded Software and Syst (HPCC, CSS, ICESS)* (pp. 1068-1075). IEEE.