Journal of Engineering and Applied Sciences 12 (Special Issue 11): 9220-9226, 2017
ISSN: 1816-949X

A Study on State of the Art in Security and Privacy Issues on Cloud Computing

[1]Abdulaziz Aldaej, [2]Ravichandran, [1]Mohammed Gulam Ahamad and [3]M.R. Ashwin Dhivakar
[1]College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Alkharj, Saudi Arabia
[2]Department of Computer Science and Engineering, Aurora Technological Research Institute, Hyderabad, India
[3]Department of Computer Science and Engineering, Jaipur National University, Jaipur, India

Abstract: The main objective of this study is not only to identify and classify the security concerns on Cloud Computing (CC) paradigm but it also depicts security management frameworks and the importance of audit and compliance functions which are relevant for the cloud platform. Security and privacy issue is one of the most important challenges in the entire discipline of cloud computing not because vulnerability is of increasing concern but because client data is managed by the third party vendors. This study describes the security capabilities that cloud services typically supply in terms of Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS) and also conjointly explains the best practices and support capabilities for Confidentiality, Integrity and Availability (CIA) of users who access cloud services. The outcome of this study will be handy reference for the enterprise managers who deal with the security and privacy of the client data which are stored on the cloud platform.

Key words: Cloud computing security, virtualization, hypervisor, data security, network security, legal and ethical issues on cloud computing

INTRODUCTION

It is well known that cloud computing paradigm has become not only the cutting edge technology of next generation of IT enterprises but it also reflects the latest trends in business to deliver dynamically scalable resources provisioned over the internet (Mell and Grance, 2011; Gonzalez *et al*., 2012; Razaque and Rizvi, 2017). Due to the advent of advanced technologies for instance, virtualization, web enabled services over the internet, utility computing, grid computing, cluster and distributed computing, the cloud computing has come to existence. The term cloud is utilized as a similitude for the internet or the web enabled services. The major advantages of adapting the cloud platform in any ventures are easily accessible services for instance, infrastructure, platform and software over the internet at any time and any place (Wang *et al*., 2010; Subashini and Kavitha, 2011; Kandukuri *et al*., 2009; Kaufman, 2009). The well known and major Cloud Service Providers (CSP) are Google, Amazon, Salesforce, Microsoft and IBM (Wang *et al*., 2010). They set up new server farms for facilitating cloud registering applications in different areas around the globe. According to the National Institute of Standards and Technology (NIST), the cloud computing system consists of five fundamental attributes, three types of administrative services and four deployment models between client consumers and Client Service Providers (CSP). The visual model of NIST working definition of Cloud Computing (CC) is depicted in Fig. 1. In general, cloud computing can be characterized into four administration models, specifically, public cloud, private cloud, hybrid cloud and community cloud (Subashini and

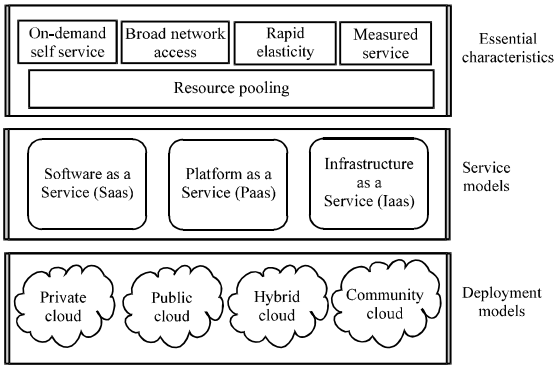

Fig. 1: Visual model of NIST working definition of cloud computing

Corresponding Author: Abdulaziz Aldaej, College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Alkharj, Saudi Arabia

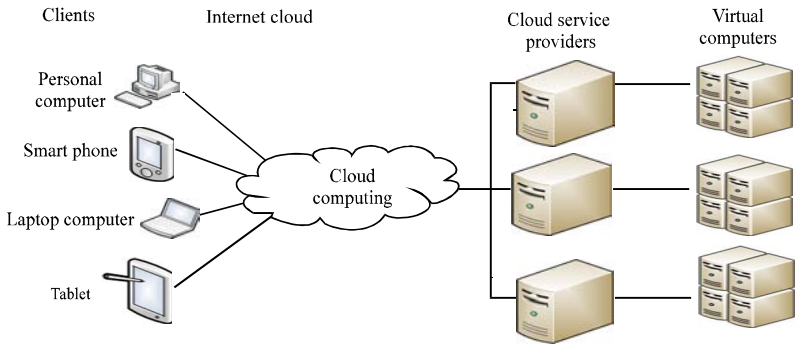

Fig. 2: Generic view of cloud computing archiitecture

Kavitha, 2011; Kandukuri *et al*., 2009). In general, cloud specialists or service providers augment to offer distributed or server computing services which can be grouped into three categories, namely, Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

It is no doubt that cloud computing promises the reduction of capital expenditure and also provides the lower maintenance and administrative costs. As a matter of fact that cloud computing paradigm not only has penetrated into our financial, social, professional, legislative and military frameworks but it also influences how the future generation of computing infrastructures are converged as a whole. In fact that cloud based computing has gotten to be necessities and dominants in every sphere of modern life but the data protection and privacy is of increasing concern due to client data is managed by the third party vendors. In any case, security and protection issue is a standout amongst the most essential, vital and important areas and challenges in the entire discipline of Cloud Computing (CC). The generic view of the cloud computer architecture is represented in Fig. 2.

Computer security is overwrought not only for protection of computer hardware components but also safe guard against abuse or unauthorized use of information disclosure, alteration or misinformation from the malicious users through intentional or unintentional actions on the cloud servers. Cloud based systems are constantly dangers of accidental blunder in addition those owing to exploitative, immoral and criminal exercises by the pernicious insiders and hackers. In cloud computing system, clients data and its multitude of crucial and mission critical applications are stored in the third party vendors that arises the data security and privacy aspects of Confidentiality, Integrity and Availability (CIA). This study depicts the security capabilities that cloud services typically supply in terms of Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) and furthermore, covers the best practices and support capabilities for handling security issues of the client data which are managed by third party vendors (Kaufman, 2009; Zissis and Lekkas, 2012; Mosa and Paton, 2016; Endo *et al*., 2016).

MATERIALS AND METHODS

Security issues on virtualization of cloud computing: It is notable that virtualization is an indispensable empowering innovation in cloud computing which permits the physical processing assets, for example, processors, main memory, storage devices and networking into pools of resources that can be made available adaptably to virtual machines. In a cloud computing paradigm, virtualization can be classified into two types, for instance, full virtualization and para-virtualization. In full virtualization, whole hardware architecture is replicated virtually for all intents and purposes. Be that as it may, in para virtualization an operating system can be run simultaneously and concurrently with other frameworks of an operating systems. Virtual Machine Monitor (VMM) is a hypervisor that abstracts the physical resources used by the different virtual machines. The VMM gives a virtual processor and other virtualized variants of framework gadgets for example, I/O devices, storage, memory, etc. (Zhang *et al*., 2010; Jaatun *et al*., 2012; Huang and Nicol, 2013).

Virtualization are mainly incorporated in the cloud platform in order to improve utilization of hardware resources, minimize the capital expenditures for computer items and serve the business dynamically in terms of adaptability and scalability. The use of virtualization technologies causes the hypervisor vulnerabilities which are the most common in the cloud technology. Side channel assault and attack is basic among various situations and is difficult to safeguard and protect the hypervisors from the malwares or network intruders. A side channel attack is one of the most widely occurred

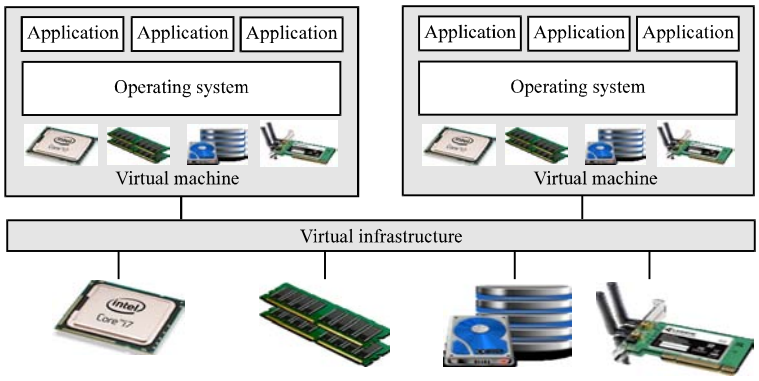

Fig. 3: Virtual machine isolation

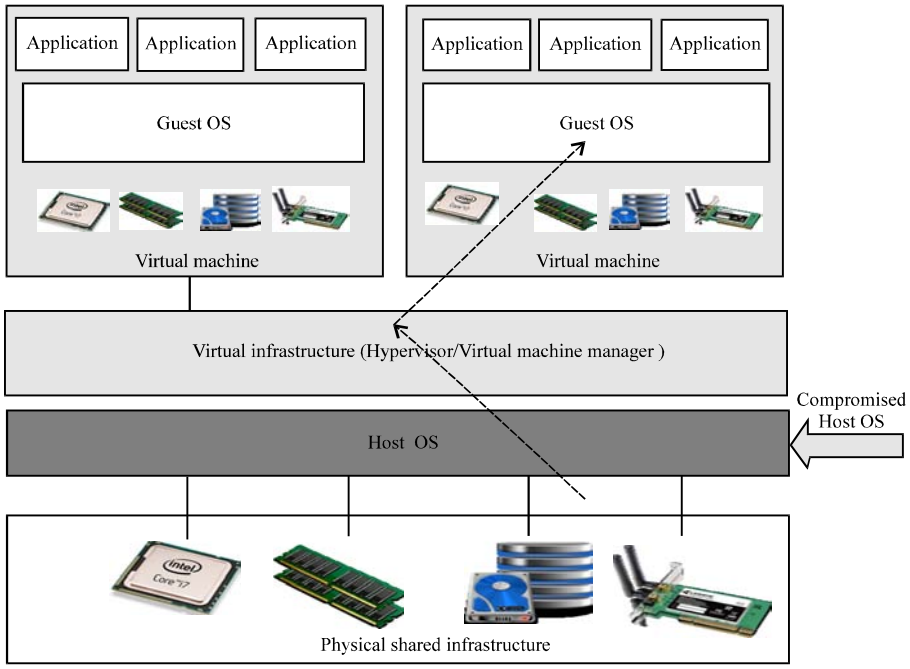

Fig. 4: Attack through the host OS

security problems among the hypervisors whenever computing resources, for example, CPU, OS, cache, memory, file system, sound and so on could be utilized as a sharing or cooperatively taking part into a system (Denz and Taylor, 2013; Ouedraogo *et al*., 2015).

Virtual machine isolation: In spite of virtual machines isolated logically, physical processing resources, for instance, CPUs, memory, storage and networking can be made available to all virtual machines. Data leaks and cross-VM attacks are easily and widely accomplished due to the common utilization of computer hardware assets (Fig. 3 and 4). It is suggested that fine grain approach to the computational resources may reduce the vulnerabilities and attacks happened on the virtualization techniques (Zhang *et al*., 2012; Liu *et al*., 2014). Due to exploitation of hypervisor vulnerabilities and lack of isolation controls among virtualized infrastructures, data leakage is the one of the common risks and attacks on the cloud platform. Mission critical data of the customer is getting affected and lost its confidentiality and integrity (Luo *et al*., 2011).

Hypervisor vulnerabilities and multi-tenancy: The hypervisor is one of the primary software components for running virtualization in the cloud platform. With help of multi-tenancy approach, Cloud Service Provider (CSP) can offer simultaneously same cloud infrastructure resources, for instance including computational resources of CPU, main and secondary storage devices, network services

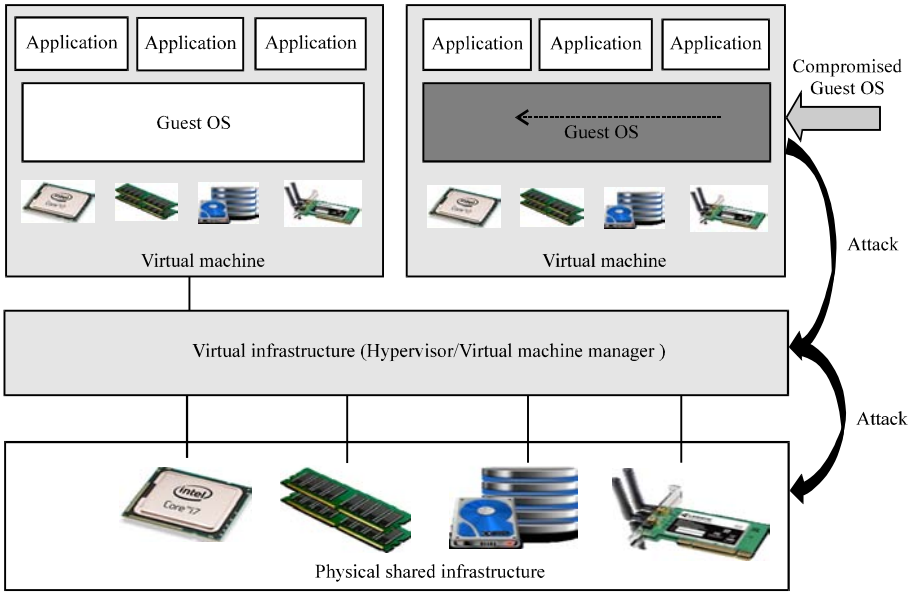

Fig. 5: Attack through the guest OS

and applications to the various customers. In the cloud platform, multi-tenancy can be achieved through the hypervisor techniques. Multi-tenancy is one of the noteworthy features of the cloud platforms. Public cloud is an unique example for resource sharing in clouds. Basically, it permits cloud suppliers to oversee resources and asset usage all the more proficiently by partitioning a virtualized, shared framework among different clients. Virtualization and multi-occupancy are the enormous issues and challenges for deploying the client data on cloud platform. Since, the cloud is a mutual and shared resources environment, cloud service providers need to ensure that each one of the tenant storage spaces are genuinely detached from each other. Clients need the ability to configure trusted virtual domains or policy-based security zones independently (Liu *et al*., 2014). Figure 4 shows how a malware of one VM sends information to another VM (Brey, 2007; Cayirci *et al*., 2016).

Cross-VM attacks: The cross VM attacks is a type of risks in which the attacker deliberately positioned a malicious VM on the same physical hypervisor platform and then accessed shared hardware and cache locations to perform a variety of side-channel attacks including Denial of Service (DoS), hardware utilization detection, remote keystroke monitoring via. timing inference and others (Zhang *et al*., 2012; Subashini and Kavitha, 2011; Nagaraju and Parthiban, 2015). Figure 5 depicts how a malware in one VM sends information to another VM through the side channel of guest OS.

RESULTS AND DISCUSSION

Data security in cloud platforms: One of the crucial security issues for most organizations who are facilitating the cloud services is to safeguard and protect client data from misuse and abuse either intentionally or accidently by the unauthorized users. The data security is not only concerned about how to protect data from corruption but it also deals with the digital privacy measures how to prevent from unauthorized access to computers, databases and websites. As indicated by the Cloud Security Alliance data security threats in cloud platforms are mainly caused by one or more of the following, for instance, virtualization of shared technology issues, cloud account hijacking, abuse, misuse and nefarious utility of cloud services, malicious insiders who steal the customers data, poorly insecure interfaces of client web browsers and permanent data loss or leakage. This study covers how data protection can be achieved in terms of Confidentiality, Availability and Integrity (CIA) which can be applied not only to cloud environments but also any solution requiring basic security levels of the digital world.

Encryption and key management: Cryptography technique is one of the most widely, commonly and frequently employed practice to safeguard and protect the sensitive data in the IT industry (Fig. 6). Though the client data is stored in the encrypted form at the third party premises of the servers, the data breaches or data leakage are common phenomenon when the clients data

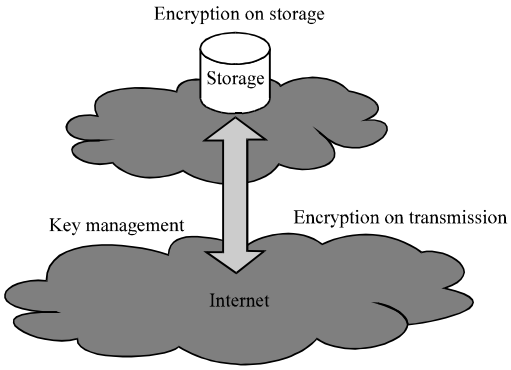

Fig. 6: Encryption on the storage management in cloud platform

is migrated across the clouds. Intruders, hackers or cyber attackers can easily penetrate into the corporate network via. poor firewall protection system. Conventional cryptography techniques may not be sufficient to safeguard the client data on the cloud platform (Mather *et al*., 2009; Halpert, 2011; Gonzalez *et al*., 2012).

Data breaches and malicious insiders: It is no doubt that the modern business models depend on heavily the usage of information technology enabled services for its core functionalities and processes in order to sustain from the cutting edge competition. The core pillar of the security services, for instance, Confidentiality, Integrity and Availability (CIA) must be safe guarded and protected the mission-critical data of the customers. An data breach is an episode in which delicate, secured or confidential data has possibly been seen, stolen or utilized by an individual unauthorized to do as such. Malicious insiders of the Cloud Service Providers (CSP) can affect the operation of the organization, for example, brand damage, financial impact and productivity losses. A safeguard against the malignant insider danger is one the critical issues for the Cloud Service Providers (CSP). The CSP must detect and defend against the misuse, abuse or malicious usage of the client data or leakage or deletion wilfully (Hashizume *et al*., 2013; Razaque and Rizvi, 2017).

Permanent data deletion: A perpetual information erasure or basic information transfer systems can be brought about by the malignant insiders of the CSP. It is an essential prerequisite that the whole obliteration or devastation of client data including log references and covered support registries must be safeguarded and protected from nefarious use (Zhang *et al*., 2012; Mosa and Paton, 2016).

Account or service hijacking: Account hijacking is a sort of data fraud in which the stolen client account is utilized for malignant or unapproved action. Account hijacking or service is also called as identity theft. Attackers can often penetrate not only the hypercritical areas of deployed cloud computing services but also the privacy of confidentiality, integrity and availability of those services are interposed. Service traffic hijacking was ascertained as the third-greatest cloud computing security risk as per the report from the cloud security alliance (Jaatun *et al*., 2012).

Network security issues on cloud computing: This area outlines the issues related with system interchanges and arrangements in regards to cloud computing frameworks. Significant issues of system security related exercises are highlighted as follows.

Spyware: Spyware is software which is used to secretly gather information about users while they browse the web over the internet. These data can be used and utilized for malicious activities. The best remedies are that install antivirus or antispyware software in both the client machines and the servers, so as to minimize the spyware and adware intrusion (Zhang *et al*., 2010; Mather *et al*., 2009).

Adware: Adware is also a type of spyware which is used to gather data about the client to show advertisements in the web program. A client's gadget could be tainted with noxious adware if there has been a spike in information utilization, the presence of new toolbars on the client's web program, redirection of the client's web inquiries to promoting sites, the presence of undesirable advertisements in fly up windows that cannot be effortlessly shut down or closed (Zhang *et al*., 2010; Mather *et al*., 2009).

Phishing: Phishing is a malicious activity which is used for sending fake messages and fraudulent e-Mails that appear to originate from honest or legitimate sources but false web sites in order to capture private information of the users or clients in the cloud platforms (Zhang *et al*., 2010; Mather *et al*., 2009).

Keyloggers: The keylogger is a pernicious technique that is used to monitor and record keystrokes of the users in the cloud platform. The keyloggers can be software or hardware devices. The gathered information can be utilized for malignant purposes. Some antivirus and antispyware programs ensure against programming keyloggers (Zhang *et al*., 2010; Mather *et al*., 2009).

Sniffing: Sniffing is a process of capturing and recording network traffic within the network of cloud platforms. Sniffing can be done by using the software or hardware that can intercept the traffic flow of the network. It is often used by hackers to intercept information (Brey, 2007; Mather *et al*., 2009).

Spoofing: Spoofing is a malicious activity which is utilized to endeavor to access a system by acting like an approved client to steal sensitive data in the cloud platform (Zhang *et al*., 2010). A spoofing attack is one of the widely used strategy in which pernicious person or attacker impersonate like legitimate user of the network system in order to penetrate the corporate network of the cloud and steal mission critical data and launch or spread malware to destroy the client data.

Firewalling: A firewall protection technique is mainly used for safe guarding the internal cloud infrastructure from the outside intruders of any untrusted network. It is observed that the exiting firewall system is not full proof from the network hackers and malicious users. Therefore, it is suggested that firewall software must be capable of handling cloud specific environments and threats (Mather *et al*., 2009).

Legal and ethical issues on compliance of cloud computing: This segment presents how to determine a key structure for limiting the lawful and ethical cumbersomeness involved in deploying the cloud computing based on the best practices across the world. The major unethical issues predominantly deal with computers in society for instance, social and political. Since, the customer information is stored in on-premises, the lawful aspects of the client computing are one of the important concerns (Gonzalez *et al*., 2012). The ethical issues are mainly focused about making choices about "what is right". The importance of ethical, legal and social responsibilities of cloud computing are highlighted in this study.

Service Level Agreements (SLA): Service Level Agreement (SLA) is ordained and enforced not only for the cloud consumers but also for the Cloud Service Providers (CSP) to make it ensured that service quality is preserved at acceptable levels in spite of the dynamic nature of the cloud environment and its features. SLA is one of the important legal agreements which contains an elucidation of the agreed cloud administration, the affirmations as to the quality of service, parameters of the level of service, arrangements and remedies for all instances of infringement (Aljoumah *et al*., 2015; Gonzalez *et al*., 2012; Razaque and Rizvi, 2017; Sharkh *et al*., 2017).

Legal issues: It is not doubt that law is necessary in all segments of society and cloud computing is no exception. The copyright, patent and trademark laws protect much of the material found on the cloud platform. However, the cyber law is exclusively used for handling the online fraudulent activities. Cyber law an evolving legal framework that governs internet activities and also covers topics ranging from copyright infringement to e-mail privacy, identity theft and interstate e-commerce via cloud platform (Gonzalez *et al*., 2012; Endo *et al*., 2016).

CONCLUSION

In this proposed study, we have highlighted the critical security contemplations and difficulties which are currently confronted in the cloud computing industry. In spite of many advantages of using the cloud platform for enterprises, security and privacy is one of the important issues before deploying the mission critical data into the cloud service provider premises. In any case one must be extremely watchful to comprehend the constraints and security dangers postured in using these technologies.

RECOMMENDATION

We conclude that cloud computing can possibly turn into a leader in advancing and economically viable IT solution in near future and that it progresses lies in standardizing cloud computing security protocols and conventions.

ACKNOWLEDGEMENTS

Researchers may need to express their gratefulness and appreciation to the organization of Prince Sattam Bin Abdulaziz University, Alkharj, Saudi Arabia and Aurora Group of colleges, Hyderabad where this research was performed.

REFERENCES

Aljoumah, E., A.F. Mousawi, I. Ahmad, A.M. Shammri and A.Z. Jady, 2015. SLA in cloud computing architectures: A comprehensive study. Intl. J. Grid Distrib. Comput., 8: 7-32.

Biancheri, C. and M.R. Dagenais, 2016. Fine-grained multilayer virtualized systems analysis. J. Cloud Comput. Adv. Syst. Appl., 5: 1-14.

Brey, P., 2007. Ethical Aspects of Information Security and Privacy. In: Security, Privacy and Trust in Modern Data Management, Petkovic, M. and W. Jonker (Eds.). Springer, Berlin, Germany, ISBN:978-3-540-69860-9, pp: 21-36.

Cayirci, E., A. Garaga, D.A.S. Oliveira and Y. Roudier, 2016. A risk assessment model for selecting cloud service providers. J. Cloud Comput. Adv. Syst. Appl., 5: 2-12.

Denz, R. and S. Taylor, 2013. A survey on securing the virtual cloud. J. Cloud Comput. Adv. Syst. Appl., 2: 2-9.

Endo, P.T., M. Rodrigues, G.E. Gonçalves, J. Kelner and D.H. Sadok *et al*., 2016. High availability in clouds: Systematic review and research challenges. J. Cloud Comput. Adv. Syst. Appl., 5: 1-2.

Gonzalez, N., C. Miers, F. Redigolo, M. Simplicio and T. Carvalho *et al*., 2012. A quantitative analysis of current security concerns and solutions for cloud computing. J. Cloud Comput. Adv. Syst. Appl., 1: 1-18.

Halpert, B., 2011. Auditing Cloud Computing: A Security and Privacy Guide. John Wiley & Sons, Hoboken, New Jersey, ISBN:978-0-470-87474-5, Pages: 207.

Hashizume, K., D.G. Rosado, E. Fernandez-Medina and E.B. Fernandez, 2013. An analysis of security issues for cloud computing. J. Internet Services Applic. 10.1186/1869-0238-4-5

Huang, J. and D.M. Nicol, 2013. Trust mechanisms for cloud computing. J. Cloud Comput., 2: 1-14.

Jaatun, M.G., C. Lambrinoudakis and C. Rong, 2012. Special issue on security in cloud computing. J. Cloud Comput. Adv. Syst. Appl., 1: 1-2.

Kandukuri, B.R., V.R. Paturi and A. Rakshit, 2009. Cloud security issues. Proceedings of the IEEE International Conference on Services Computing, September 21-25, 2009, Bangalore, India, pp: 517-520.

Kaufman, L.M., 2009. Data security in the world of cloud computing. IEEE Secur. Privacy, 7: 61-64.

Liu, F., L. Ren and H. Bai, 2014. Mitigating cross-VM side channel attack on multiple tenants cloud platform. J. Comput. Acad., 9: 1005-1013.

Luo, S., Z. Lin, X. Chen, Z. Yang and J. Chen, 2011. Virtualization security for cloud computing service. Proceedings of the 2011 International Conference on Cloud and Service Computing, December 12-14, 2011, IEEE, Hong Kong, China, ISBN:978-1-4577-1637-9, pp: 174-179.

Mather, T., S. Kumaraswamy and S. Latif, 2009. Cloud Security and Privacy. O'Reilly Media, Sebastopol, California, USA., ISBN:9780596807504, Pages: 312.

Mell, P. and T. Grance, 2011. The NIST definition of cloud computing recommendations of the national institute of standards and technology. Nist Spec. Publ., 145: 1-7.

Mosa, A. and N.W. Paton, 2016. Optimizing virtual machine placement for energy and SLA in clouds using utility functions. J. Cloud Comput. Adv. Syst. Appl., 5: 2-17.

Nagaraju, S. and L. Parthiban, 2015. Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway. J. Cloud Comput. Adv. Syst. Appl., 4: 1-22.

Nikravesh, A.Y., S.A. Ajila and C.H. Lung, 2017. An autonomic prediction suite for cloud resource provisioning. J. Cloud Comput., 6: 1-20.

Ouedraogo, M., S. Mignon, H. Cholez, S. Furnell and E. Dubois, 2015. Security transparency: The next frontier for security research in the cloud. J. Cloud Comput. Adv. Syst. Appl., 4: 1-14.

Razaque, A. and S.S. Rizvi, 2017. Privacy preserving model: A new scheme for auditing cloud stakeholders. J. Cloud Comput. Adv. Syst. Appl., 6: 1-17.

Sharkh, M.A., A. Shami and A. Ouda, 2017. Optimal and suboptimal resource allocation techniques in cloud computing data centers. J. Cloud Comput. Adv. Syst. Appl., 6: 1-17.

Subashini, S. and V. Kavitha, 2011. A survey on security issues in service delivery models of cloud computing. J. Network Comput. Appl., 34: 1-11.

Wang, C., Q. Wang, K. Ren and W. Lou, 2010. Privacy-preserving public auditing for data storage security in cloud computing. Proceedings of the 2010 IEEE Conference on INFOCOM, March 14-19, 2010, IEEE, San Diego, California, pp: 1-9.

Zhang, Q., L. Cheng and R. Boutaba, 2010. Cloud computing: State-of-the-art and research challenges. J. Internet Serv. Applic., 1: 7-18.

Zhang, Y., A. Juels, M.K. Reiter and T. Ristenpart, 2012. Cross-VM side channels and their use to extract private keys. Proceedings of the 2012 ACM Conference on Computer and Communications Security, October 16-18, 2012, Raleigh, NC., USA., pp: 305-316.

Zissis, D. and D. Lekkas, 2012. Addressing cloud computing security issues. Future Gener. Comput. Syst., 28: 583-592.