2015 Fifth International Conference on Advanced Computing & Communication Technologies

Security Concerns and Countermeasures in Cloud Computing Paradigm

Meena Kumari
PhD Research Scholar, Department of Computer Science and Applications
Kurukshetra University, Kurukshetra,
Haryana,India.
email: sanger.meena@gmail.com

Rajender Nath
Professor, Department of Computer Science and Application
Kurukshetra University, Kurukshetra,
Haryana, India.
email: rnath@kuk.ac.in

***Abstract* - Since the inception in 2006, cloud computing has been a hot researching area of computer network technology. Some giant companies are offering the cloud services now. Migrating data to the cloud remains a tempting trend from a financial perspective but there are several other aspects that must be taken into account before it is decided to do so. One of the most important aspects is security. Cloud computing security refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. This work will enable researchers and security professionals to know about users and vendors concerns and identifies relevant countermeasures to strengthen security and privacy in the Cloud environment.**

Keywords- availability; cloud computing; cloud security; confidentiality; elasticity; integrity.

I. INTRODUCTION

The importance of cloud computing is increasing and it is receiving a growing attention in the scientific and industrial communities. A study by Gartner [2] considered cloud computing as the first among the top 10 most important technologies and with a better prospect in successive years by companies and organizations. The cloud computing is a computing model that provides the uniform access to wide area distributed resources on demand [3].It entrusts remote services. In this demanding world the reason to adopt cloud computing over standard IT deployments is flexibility, stability, rapid provisioning, reliability and scalability. The utilities can be leased and released by user through Internet on demand basis. Moving data to the cloud presents the enterprise with a number of risks, which include securing critical information like the protection of intellectual property, trade secrets, personally identifiable information that could fall into the wrong hands. In the cloud environment, the enterprise may have little or no visibility to storage and backup processes and little or no physical access to storage devices at the cloud computing provider. Moreover, because the data from multiple customers may be stored in a single repository, forensic inspection of the storage media and a proper understanding of the access and deletion is a significant challenge.

This paper analyzes and discusses the security issues involving data, application, and virtualization technologies and countermeasures to these issues present in cloud computing.

The rest of the paper is organized as follows: Section II gives the review method and Section III provides cloud computing overview. Section IV discusses security threats present in the cloud and their countermeasures in Section V. Section VI describes the limitations of our work and possible future work and Section VII presents concluding remarks.

II. REVIEW METHOD

This study reviews and classifies and the publications according to the security area they address. This section set the boundaries and the scope of the literature reviewed. we searched each of the major research databases for computer science, such as the ACM Digital Library, IEEE Xplore, Springer Link, ScienceDirect and Google Scholar, for the following keywords: cloud computing, cloud security, security in cloud computing. The searches from the five target databases returned over 100 papers. The titles and abstracts of these papers were read and considered as relevant all publications that complied with the following criteria:

Inclusion criteria: Introduction to cloud computing and cloud computing security must be the major topic or one of the major topics of the publications. 40 papers satisfied this criterion and were included for review.

Exclusion criteria: papers pertaining to a very specific context (e.g. railways, healthcare, national security, etc) are excluded from the study as this paper is interested in more general security requirements and solutions. Journal articles that were not accessible online are also excluded.

2327-0659/15 $31.00 © 2015 IEEE
DOI 10.1109/ACCT.2015.80

The papers were split into categories based on their main focus. The categories are general introductions and Technological aspects. The technological category was further broken down into papers that dealt with different security issues along with their solutions. Table 1 provides an overview of the papers reviewed along with their categories.

Table 1: Overview of reviewed literature

Category		Authors
General Introductions and Definition		P.Mell et al., Mladen A. Vouk, Nariman Mirzaei, Jeffrey Shafer, Ilyas Iyoob et al. and Vaquero et al.
Security Issues	Governance	Wayne jenson et al.,Gonzalez Nelson *et al.*
	Compliance	Wayne jenson et al., Haifeng Fang et al.
	Multitenancy	Huaglory Tianfield , Akhil Behl et al.
	Trust	Hashizume keiko et al.
	Virtualization related issues	Dawoud W et al., Ranjith P et al.,” J. Kirch, Hans P. Reiser, T. Garfinkel and M. Rosenblum.
	Data related issues	Hashizume keiko et al.
	Attacks	Wayne Jansen et al., Hans P. Reiser and Hashizume keiko et al.
	Information Integrity and Privacy	Behl Akhil et al.
Security solutions	Governance	Meetei Mutum Zico et al.,Shaikh Farhan Bashir et al.,Zhiyun Guo et al.
	Compliance	Tripathy Alok et al., *Sotto Lisa J. et al.*
	Multitenancy	Tripathy Alok et al.,Sun Dawei et al.,
	Trust	Lyle John et al., Ateniese, G.et al., Santos N et al.
	Virtualization related issues	Haifeng Fang et al., Wu H et al.
	Data related issues	Cheung David W, Tan Yubo et al., Bethencourt John et al.
	Attacks	Chen Zhen et al., Tsai Chang-Lung et al., *D Asha et al.*
	Information Integrity and Privacy	H. Chang et al., Lar Saleem-ullah et al.,Chang Hyokyung et al.

III CLOUD COMPUTING DEFINITION

This section provides an overview of cloud computing definitions. Cloud computing is under development, there are no widely accepted unified definition. In different stages of development or from a different perspective has a different understanding on the cloud. U.S. National Institute of Standards and Technology (NIST) definition is one of the clearest and most comprehensive definitions of cloud computing and is widely referenced .The NIST definition summarizes cloud computing *as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction* [1]. This cloud model promotes availability and is composed of five essential characteristics, three delivery models, and four deployment models."[4-8].

Vaquero et al.[9] studied 22 definitions of cloud computing and proposed the following definition:

Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically re-configured to adjust to a variable load (scale), allowing also for optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs.

According to Muhammad Baqer Mollah et al. [11] *Cloud computing is TCP/IP based high development and integrations of computer technologies such as fast microprocessor, huge memory, high-speed network and reliable system architecture.*

Buyya [15] defined Cloud as *A Cloud is a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements* *established through negotiation between the service provider and consumers.*

Although there are still many internet forum and blog discussions on what cloud computing is and is not, the NIST definition seems to have captured the commonly agreed aspects of cloud computing that are mentioned in most of the academic papers published in this area.

IV SECURITY ISSUES IN CLOUD COMPUTING

The remainder of this paper reviews the research that describes security aspects of research in cloud computing. Below, the different security issues are explained and the 45 papers selected to be included in the review are classified as addressing one of the issues. Table 2 provides a description of terms pertaining to cloud security issues as described by various publications.

Table 2: Security Issues in cloud computing.

Sr. No.	Issues	Description
1	Governance	implies control and oversight by the organization over policies and standards for application development and IT service acquisition [10][13]
2	Compliance	Cloud computing providers may refuse to external audits and security certifications[23]
3	Trust	the customer's has to trust that the organization is capable of providing the required services accurately and infallibly [22].
4	Multitenancy	threat of information leakage and exploitation during the share of application and hardware [24]
5	Vulnerabilities in Virtual Machines [19][20][21]	a)Possible covert channels in the collocation of VMs [18] b) Unrestricted allocation and deallocation of resources with VMs [16] c) Uncontrolled Migration - VMs can be migrated from one server to another server due to fault tolerance, load balance, or hardware maintenance [17] d) Uncontrolled snapshots – VMs can be copied in order to provide flexibility [12], which may lead to data leakage e) Uncontrolled rollback could lead to reset vulnerabilities - VMs can be backed up to a previous state for restoration [44], but patches applied after the previous state disappear f) VMs have IP addresses that are visible to anyone within the cloud - attackers can map where the target VM is located within the cloud (Cloud cartography)[22]
6	Data related issues	a) Data loss- while it is being transferred, stored, audited or processed . b) Data Scavanging- Attacker may recover deleted data.
7	Attacks	a) DOS/DDOS- saturating the target with bogus requests to prevent it from responding to legitimate requests [10]. b) Backdoor Channel - allows hackers to gain remote access to the compromised system [10]. c) Spoofing/ Sniffing - A malicious VM can listen to the virtual network or even use ARP spoofing to redirect packets from/to other VMs [20]. d) Service hijacking- attacker can gains access to a user's credential and can perform malicious activities [22].
8	Information Integrity and Privacy issue	a)Absence of authentication and authorization and accounting controls [24] b)No management of encryption/decryption keys (Key Management) [24]

V COUNTERMEASURES FOR SECURITY CONCERNS

This section briefly describes some countermeasures to above mentioned security issues.

a) *Governance*

- Cloud Security Alliance has created a cloud Governance, Risk Management and Compliance (GRC) toolkit, supported by checklists and questionnaire, for cloud migration audit [25][26].
- Zhiyun Guo et al. [27] have proposed a cloud based governance model that marks out a path which will guide the enterprise into the cloud in a controlled and secure manner.

b) *Compliance*

- US Federal and other international laws such as the Electronic Communication Privacy Act (ECPA) can govern concerns for data privacy in cloud. Sarbanes-Oxley Act (SOX) and HIPAA (Health Insurance Portability and Accountability Act) FISMA - Federal Information Security Management Act and FIPS - Federal Information Processing Standard are other well-known regulations [28].
- It is important to ensure that cloud computing providers are obliged to undergo external audits and security certifications. One popular auditing guideline is the SAS-70 [29].

c) *Trust*

- Trusted Computing Groups (TCG) is developing tools that will help IT users access the trustworthiness of suppliers, enable compliance, monitor in real time and implement standards-based cloud security solutions [30][32].
- Proofs of Retrievability (PoR) give customer some semblance of assurance that once data is stored in a public cloud, it will be eventually retrievable [31].
- Trusted cloud computing platform TCCP is proposed in [33] which enables providers to offer closed box execution environments, and allows users to determine if the environment is secure before launching their VMs.

d) *Multitenancy*

- Using VMs for each tenant [34].
- Cachinet al.[28] has proposed a Byzantine fault-tolerant replication protocol.
- An organization porting its data and processes to cloud should have their policies and security procedures ported alongside the data to ensure that their data lies in isolation to the data of other tenants [24].
- There should be a level of isolation amongst tenants data (at rest ,and in transition).

e) *Vulnerability in Virtualization*

- VMGuard [23] is an integrity monitoring and detecting system which utilizes a special VM, Guard Domain, and runs on each physical node to monitor the co-resident management VMs.
- Dawei Sun et al. has remarked that System-level virtualization can improve dependability and enhance security of cloud systems for a number of reasons and the three major justifications are system consolidation, isolation and live migration [34].
- Wu and et al. [35] presents a virtual network framework that secures the communication among virtual machines and prevent VMs from sniffing and spoofing.

f) *Data related issues*

- Bessani et al. [33] present a virtual storage cloud system called DepSky system which addresses the availability and the confidentiality of data in their storage system by using multi-cloud providers [34].
- Encryption/Decryption Procedures like AES, DES , RSA can be incorporated on data at rest or in transition.
- David W. Cheung [40] has proposed a model SCONEDB (Secure Computation ON an Encrypted DataBase) which incorporates the attacker capability as a distinct component and uses it to measure the security level of the encryption scheme.
- Yubo Tan et al. [41] has proposed a Full Homomorphic encryption algorithm [42] [43].
- M.G. Jaatun et al.[44] has remarked that by adopting federated identity management together with hierarchical identity-based cryptography (HIBC), not only the key distribution but also the mutual authentication can be simplified.
- John Bethencourt et al.[45] has presented a Ciphertext-Policy Attribute-Based Encryption techniques through which encrypted data can be kept confidential even if the storage server is untrusted.

g) Information Integrity and Privacy issue

- Use of DAC (Discretionary Access Control), MAC (Media Access Control), and RBAC (Role-Based Access Control) [38].
- Use of security standard specifications such as Security Assertion Markup Language (SAML), Extensible Access Control Markup Language (XACML), and XML Encryption, Key Management Specification (XKMS) to ensure integrity, confidentiality, authentication and authorization [36].
- Technologies like Id/password, Public Key Infrastructure, multi-factor authentication, SSO (Single Sign On) [39], MTM (Mobile Trusted Module), and i-Pin can be used to authenticate a user [37].

h) Attacks

- Firewalls, Intrusion Detection Systems (IDS), and Anti-Virus Gateway are now widely deployed in edge networks to protect end-systems from attack.
- A collaborative network security management system is proposed by [46] with an effective collaborative Unified Threat Management (UTM) and traffic probers. Zhen Chen et al. has proposed a design and implementation of a cloud-based security center for network security forensic analysis. They propose using cloud storage to keep collected traffic data and then processing it with cloud computing platforms to find the malicious attacks.
- A dynamic intrusion detection system (IDS) combined with honey net is proposed by [47] to verify the system's robustness.
- DDoS filtering technique can be used to detect and prevent the HTTP and XML DDOS attacks [48].

VI LIMITATIONS AND FUTURE RESEARCH DIRECTIONS

The main limitations of this work could be bias in the selection of papers to be included, and in categorization. To help to ensure that the process of selection was unbiased, this paper has developed a review protocol, by defining its search strategy and paper selection process. All the necessary precautions were taken to select research papers according to their main issue that they emphasize but there might be chances that a clear boundary cannot be maintained if more than one or two issues were addressed. We classified the publications according to the security area that was most elaborated upon; this does not mean that the rest of the security issues addressed by the same article are not valuable or significant.

For future work, this paper has identified few areas which are still unattended in cloud computing security such as auditing, side channels and migration of data from one cloud to another. Emphasis has always been on fast performance and low cost but the quality of service has not been considered. The research on mobile platform with respect to cloud computing is another open research issue.

VII CONCLUSION

With the massive growth in cloud computing adoption, the security attracted the attention of researchers and practitioners but still it has not been addressed completely. This paper represents a milestone for the day where cloud computing security issues can be listed in one comprehensive document together with its solutions. This paper identifies top security concerns of cloud computing, these concerns are Data loss, Governance and compliance, Trust, Virtualization vulnerabilities and various attacks. It also summarizes various countermeasures which can be adopted to overcome above mentioned security issues. This study provides a pillar to researcher and practitioner where they can stand and further identify the issues and enhance cloud-computing security.

REFERENCES

1. Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing (ver. 15)", National Institute of Standards and Technology, Information Technology Laboratory, October 7, 2009.
2. Gartner Inc.," Gartner identifies the Top 10 strategic technologies for 2011",[Online]: http://www.gartner.com/it/page.jsp?id=1454221. Accessed: 15-dec-2014.
3. Verma Amandeep, Kaushal Sakshi,"Cloud Computing Security Issues and Challenges: A Survey", Springer-Verlag Berlin Heidelberg, ACC 2011, Part IV, CCIS 193, pp. 445–454, 2011.
4. Caroline Kvitka, "Clouds Bring Agility to the Enterprise", [Online] Available at: http:// www.oracle.com /technology/ oramag/ oracle/ 10-mar/o20interview.html, Accessed: 15-dec-2014.
5. You Pengfei, Peng Yuxing , Liu Weidong , Xue Shoufu ," Security Issues and Solutions in Cloud Computing", In: Proc. Of 32nd International Conference on Distributed Computing Systems Workshops, 2012.

6. Iyoob1 Ilyas , Zarifoglu Emrah , Dieker A.B.," Cloud Computing Operations Research", Gravitant and University of Texas at Austin, 2008.
7. Shafer Jeffrey," I/O Virtualization Bottlenecks in Cloud Computing Today", In: Proc. Of Second Workshop on I/O Virtualization (WIOV '10), March 13, 2010.
8. Vouk Mladen A, "Cloud Computing – Issues, Research and Implementations", Journal of Computing and Information Technology - CIT 16, 2008, pp 235–246.
9. Vaquero," A break in the clouds: towards a cloud definition", SIGCOMM Comput. Commun. Rev. 39, 1, 50-55,2008.
10. Wayne Jansen , Grance Timothy,"Guidelines on Security and Privacy in Public Cloud Computing",National Institute of Standards and Technology,2011.
11. Mollah Muhammad Baqer , Islam Kazi Reazul, Islam Sikder Sunbeam," Next Generation of Computing through Cloud Computing Technology" In: Proc. Of 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), 2012.
12. Tianfield Huaglory,"Security issues in Cloud Computing", In : Proc of IEEE International Conference on Systems, Man, and Cybernetics,Korea,2012.
13. Gonzalez Nelson , Miers Charles , Redígolo Fernando , Carvalho Tereza , Simplicio Marcos*," A quantitative analysis of current security concerns and solutions for cloud computing", Journal of Cloud Computing: Advances, Systems and Applications Springer,* 2012.
14. Zissis Dimitrios , Lekkas Dimitrios," Addressing cloud computing security issues", SciVerse ScienceDirect,2012.
15. Buyya,"Cloud Computing and emerging IT platforms: vision, hype, and relatity for deliverling computing as the 5th utility", Future Generation Computer System 25(6), 599–616 ,2009.
16. Winkler V," Securing the Cloud: Cloud computer Security techniques and tactics", Elsevier Inc, Waltham, MA, 2012.
17. Dawoud W," Infrastructure as a service security:Challenges and solutions",In: Proc. of 7th International Conference on Informatics and Systems (INFOS), Potsdam, Germany. IEEE, 2010, pp 1–8.
18. Ranjith P," On covert channels between virtual machines" Journal in Computer Virology Springer, 2012, pp 85–97.
19. J. Kirch," Virtual Machine Security Guidelines Version 1.0" The Center for Internet Security, September 2007.
20. Hans P. Reiser,"Security Challenges with Virtualization",December 2009.
21. T. Garfinkel ," When virtual is harder than real:security challenges in virtual machine based computing environments".In HOTOS'05: Proceedings of the 10th conference on Hot Topics in Operating Systems, pages 20–20, Berkeley, CA, USA, 2005. USENIX Association.
22. Hashizume keiko, Rosado David G , Fernández-Medina Eduardo and Fernandez Eduardo B ,"An analysis of security issues for cloud computing" Journal of Internet Services and Applications, 2013,pp 1-13.
23. Haifeng Fang, "VMGuard: An Integrity Monitoring System for Management Virtual Machines", In : Proc of IEEE 16th International Conference on Parallel and Distributed Systems (ICPADS 2010), December, 2010.
24. Behl Akhil, Behl Kanika,"An analysis of cloud computing security issues",IEEE, 2012.
25. Meetei Mutum Zico," Security Issues in Cloud Computing",In:Proc. Of 5th International Conference on BioMedical Engineering and Informatics, 2012.
26. Shaikh Farhan Bashir , Haider Sajjad," Security Threats in Cloud Computing", In : Proc of 6th International Conference on Internet Technology and Secured Transactions, Abu Dhabi, United Arab Emirates, 11-14 December 2011.
27. Zhiyun Guo," A Governance Model for Cloud Computing",In: Proc of International Conference on Management and Service Science (MASS), August,2010.
28. Tripathy Alok, Mishra Abhinav" Cloud Computing Security Considerations",IEEE, 2011.
29. *Sotto Lisa J.,* Treacy Bridget C., and McLellan Melinda L.," Privacy and Data Security Risks in Cloud Computing*",* Electronic Commerce & Law Report, 2010.
30. Lyle John," Trusted Computing and Provenance: Better Together", In: Proc. of the Workshop on Hot Topics in Cloud Computing, San Diego, 2009.
31. Ateniese, G,"Provable Data Possession in Untrusted Stores",In: Proceedings of the 14th ACM conference on Computer and Communication Security, 2007.
32. Trusted computing group, "Cloud Security", [Online] Available at: <https://www.trustedcomputinggroup.org/solutions/cloud_security>, accessed: 17-dec-2014.
33. Santos N," Towards Trusted Cloud Computing", In: Proceedings of the 2009 conference on Hot topics in cloud computing, San Diego, California. USENIX Association Berkeley, CA, USA, 2009.
34. Sun Dawei, Chang Guiran , Tan Chunguang , and Wang Xingwei , "Enhancing Security by System-Level Virtualization in Cloud Computing Environments", Springer-Verlag Berlin Heidelberg, 2011.
35. Wu H, Ding Y, Winer C, Yao L (2010) Network Security for virtual machine in Cloud Computing. In: 5th International conference on computer sciences and convergence information technology (ICCIT). IEEE Computer Society Washington, DC, USA, pp 18–21
36. H. Chang, Jang Changbok, Ahn Hyosik, and Choi Euiin," Authentication Platform for Provisioning in Cloud Computing", Springer-Verlag Berlin Heidelberg, 2011.
37. Lar Saleem-ullah, Liao Xiaofeng and Abbas Syed Ali," Cloud Computing Privacy & Security Global Issues, Challenges, & Mechanisms", In: Proc. of 6th International ICST Conference on Communications and Networking in China (CHINACOM), 2011.

38. Chang Hyokyung , Choi Euiin," User Authentication in Cloud Computing", Springer-Verlag, Berlin Heidelberg ,2011.
39. Zamani Mazdak ," A Survey on Security Issues of Federated Identity in the Cloud Computing", In : Proc of IEEE 4th International Conference on Cloud Computing Technology and Science,2012.
40. Cheung David W.," Security on Cloud Computing, Query Computation and Data Mining on Encrypted Database",IEEE, 2012.
41. Tan Yubo, Wang Xinlei,"Research of Cloud Computing Data Security Technology", IEEE, 2012.
42. Craig Gentry," Fully Homomorphic Encryption Using Ideal Lattices", In: Proc. Of *the 41st ACM Symposium on Theory of Computing (STOC)*, 2009.
43. Zhao Feng, Li Chao,Liu Chun Feng," A cloud computing security solution based on fully homomorphic encryption",*In: Proc. of ICACT,2014.*
44. M.G. Jaatun , "Strengthen Cloud Computing Security with Federal Identity Management",CloudCom , pp. 167–177, 2009.
45. Bethencourt John, Amit Sahai,Brent Waters," Ciphertext-Policy Attribute-Based Encryption",IEEE,2011.
46. Chen Zhen , Han Fuye, Cao Junwei, Jiang Xin, and Chen Shuo," Cloud Computing-Based Forensic Analysis for Collaborative Network Security Management System", Tsinghua Science And Technology, Volume 18, Number 1, February 2013 , pp40-50.
47. Tsai Chang-Lung , Lin Uei-Chin , Chang Allen Y. ,Chen Chun-Jung," Information Security Issue of Enterprises Adopting the Application of Cloud Computing",IEEE,2011.
48. D Asha , *R.Chitra,"* Securing cloud from ddos attacks using intrusion detection system in virtual machine**",**IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013.