Analysis and Countermeasures for Security and Privacy Issues in Cloud Computing

Abdul Raoof Wani, Q. P. Rana and Nitin Pandey

Abstract Cloud computing is having the capacity to dispose off the prerequisites for setting up high-cost computing framework and promises to provide the flexible architecture which is accessible from anywhere. The data in the cloud computing resides over an arrangement of network resources which enables position of the requirements for setting up costly data centers framework and information to be acquired to via virtual machines, and these serves might be arranged in any piece of the world. The cloud computing environment is adopted by a large number of organizations so the rapid transition toward the clouds has fueled concerns about security perspective. There are numbers of risks and challenges that have emerged due to use of cloud computing. The aim of this paper is to identify security issues in cloud computing which will be helpful to both cloud service providers and users to resolve those issues. As a result, this paper will access cloud security by recognizing security requirements and attempt to present the feasible solution that can reduce these potential threats.

Keywords Cloud computing · Cloud attacks · Security issues
Cloud security threats

A. R. Wani (✉) · N. Pandey
Amity University Noida, Noida, India
e-mail: wanirauf@gmail.com

N. Pandey
e-mail: Npandey@gmail.com

Q. P. Rana
Jamia Hamdard University, New Delhi, India
e-mail: qprana@jamiahamdard.ac.in

P. K. Kapur et al. (eds.), *System Performance and Management Analytics*,
Asset Analytics, https://doi.org/10.1007/978-981-10-7323-6_4

1 Introduction

Internet is the driving force behind various technologies but one of the discussed among all of them is cloud computing. It is still an advancing innovation technology that exchanges current innovating technology and figuring thoughts into utility like arrangements. The relocation diminishes time and cost of creation and offers better execution and unwavering quality [1]. Cloud computing is well defined as the convenient, on demand, and network access to the pool of resources like network servers, storage devices, and services that can quickly provisioned and released with nominal management effort [2]. The advantages of distributed computing incorporate diminishing the equipment and support cost, accessibility around globe, adaptability, and to a great degree mechanized process. It conveys unfathomable advantages to both individuals and ventures by decreasing the requirement for client association by concealing specialized points of interest, for example, updates, licenses, and support from its clients. Cloud can like wises provide improved safety over single-server arrangements and subsequently cloud totals resources and permits licensed security individual while as the typical organizations are restricted with system and network admin who will not be well learned about cybersecurity issues. Cloud computing can be stronger in distributive denial of service attacks in view of the availability of assets and flexibility of design.

2 Related Work

Analysts research on perceiving cloud issues, shortcomings, threats, and other security and protection matters to give countermeasures as plans, approaches, and architectures [3–5]. Various case studies [6–9] have led research on security in cloud computing and matters concerning single property, for example, information reconciliation, confirmation, shortcomings, and reviewing. Different scientists offer reviews [10–12] that cover the different zones and different security issues and resolutions. The joining of mobiles with cloud computing because of the utilization of cell phones has another security challenge identified with those that are related to ad hoc and sensor networks [13, 14]. The authors presented reviews on cloud security necessities like privacy, integrity, transparency, accessibility, and accountability.

3 Issues and Categories

This paper classifies the issues in the following categories (Tables 1 and 2).

Table 1 Cloud computing security categories

Category	Description
Standards	Criteria required to take safety efforts in cloud computing with a specific end goal to maintain safety and avoid attacks
Network issues	Incorporates issues in network, for example, connection accessibility, Denial of Service (DoS), flooding issues, web convention susceptibilities, and so on
Access control	Incorporates check and get to control and catches matters that influence confidentiality of client data and information storage
Data	Incorporates information linked to security matters including information development, quality, security, and warehousing
Cloud infrastructure	Incorporates issues that are precise to the cloud framework

Table 2 Cloud computing security issues and classifications

Category	Issues
Security standards	✓ Deficiency of security measures ✓ Compliance dangers ✓ Deficiency of looking into ✓ Lack of lawful components (service-level understanding) ✓ Trust
Network	✓ Appropriate establishment of system firewalls ✓ Security setups ✓ Internet protocol shortcomings ✓ Internet Requirements
Access control	✓ Accounts ✓ Malicious insiders ✓ Validation ✓ Private client access ✓ Browser Safety
Data	✓ Redundancy of information and data ✓ loss and data and information ✓ location of data and information ✓ Privacy of data and information ✓ Protection of information ✓ Data Availability
Cloud infrastructure	✓ Uncertain interface of API ✓ Quality of administration ✓ Allocation of technical defects ✓ Dependability of Suppliers ✓ Security misconfiguration ✓ Multi-occupancy ✓ Server Site and Backup

4 Attacks and Countermeasures

We have evaluated some of the known attacks in cloud computing and tried to find possible countermeasures to these known attacks.

4.1 Theft of Service

The theft of service attack [15] exploits the weaknesses in the scheduler of some hypervisor. This attack is recognized when scheduling mechanism is invoked by the hypervisor that fails to identify the account. The hacker guarantees that the process is certainly not scheduled. The common events of this attack are by means of cloud computing sources like human resources for a lengthy time and keeping it secreted from a dealer and using cloud computing means like storage or operating system platform for extended time without repeating it in billing cycle.

The countermeasures to this issue are given by Zhou et al. in [16] by altering the scheduling and changing the scheduling processes as well as checking policies and time intervals by means of exact scheduling, uniform scheduling, passion scheduling, and Bernoulli scheduling.

4.2 Denial of Service Attack

Out of the grave issues in the cloud security, denial of service attack is the most serious one. The attacks are at ease to perform and problematic for security professionals to deal with DDoS attacks that are more damaging than DoS attacks because there is no deterrence mechanism to avoid them.

Karnwal et al. [17] give a plan called cloud defender which deals with sensor filtering, hop count filtering, ip divergence filtering, puzzle resolving, and double signature filtering, yet the issue is that it needs an evidence and particle proof and is built on supposition.

4.3 Malware Injection

The malware injection issue accounts to a deployed replica of victims service instance uploaded by hacker; thus, the service requirements are processed within malicious instance. The hacker exports its private access to attack service security domain and acquires access to the customer data. The challenge is not only to identify malware injection but also ability to define the specific node on which hacker has loaded for malicious purpose [18].

The countermeasure is given by Oberheide et al. in [19] called Cloud Av which provides two features antivirus as a service and N-version defense. The authors prove the efficiency of Cloud Av by validating in cloud environment which provides improved detection of malicious software, improved forensic capabilities, and novel threat discovery approach.

4.4 Phishing Attacks

It is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack, or the revealing of sensitive information.

Cloud service alliance stated that CSP does not maintain adequate control over system in order to escape such attacks but CSA offers some precautionary measures such as registration procedure, security identity check technique, and improved monitoring skills [20].

4.5 Botnet Attacks

In this type of attack, the attackers do not reveal their identities to decrease the chance of discovery and traceback. This is accomplished by targeting victim by sequence of other hosts named stepping stone which is recruited through illegal botnets.

The countermeasures of stepping stone and botnet are by recognizing a specific host which is a stepping stone. The finding work is built on the hypothesis of relationship between licensing and outbound traffic of likely stepping stone host.

4.6 Audio Steganography Attacks

Audio steganography attacks are one of the grave attacks to cloud storage system. Audio steganography benefits customers to hide their top-secret information with normal audio records. The user communicates secret info via transferring media files which seem to be regular media records. Attackers are able to trick the present security mechanism by hiding their malicious cipher in sound records and direct it to target's server [21].

Liu et al. in [22] performed an investigation of audio steganography attacks on cloud storage system. The key is to investigate the hiding place of audio records beneath storage system by grayscale steganalysis technique.

4.7 VM Rollback Attacks

The VM part in cloud computing is most susceptible to issues. In VM rollback attack, an attacker takes benefit of prior snaps and run it without taking client into account and then erases history and again runs the similar or changed snap. The hacker launches brute force attack to give login and password for virtual machine and even if the guest operating system has restrictions on the amount of efforts such as blockade as user [22].

Szefer et al. [23] provided a design named hyperwall to cope with the hypervision susceptibilities. The hyperwall disables the suspended rescue functions of the hypervision.

5 Discussion

Out of the lots of challenges faced by cloud computing, security is still one of the biggest challenges introducing security resolutions like IDs, firewalls, contract out the personality supervision framework, and introducing antivirus, and so forth are costly and influence execution. The significant security research work lies in giving good security techniques in doing as such with minimal resources and without decline performance [23, 24].

This helps in providing the complete study of attacks in cloud, forming dependencies, and co-relating vulnerabilities across various cloud companies. It helps us to deliver protective measures as well as protection tools. This paper identifies few parts that are still not given attention in cloud computing such as checking and relocation of data from cloud to other. Security procedures must be dynamic and autonomous and should be implanted in cloud architecture for better results.

6 Conclusion

The adaption of clouds is rising day by day. With the gigantic evolution of cloud computing, the security of cloud remains still a big challenge and has not been addressed completely. In this work, we identified the security issues and tried to provide countermeasures and comparative analysis of effectiveness of the prepared solutions.

We identified the areas that are still unattended such as auditing and migration. We identified that emphasis should not only be given only on fast performance but quality of service should be considered seriously.

References

1. Tripathi, A., & Mishra, A. (2011). Cloud computing security considerations. In *Proceedings of the 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)* (pp. 1–8), Xi'an, China, 14–16 September 2011.
2. Mill, P., & Grace, T. (2011). The NIST definition of cloud computing, January 2011.
3. Wang, J.-J., & Mu, S. (2011). Security issues and countermeasures in cloud computing. In *Proceedings of the 2011 IEEE International Conference on Grey Systems and Intelligent Services (GSIS)* (pp. 843–846), Nanjing, China, 15–18 September 2011.
4. Houmansadr, A., Zonouz, S. A., & Berthier, R. (2011). A cloud-based intrusion detection and response system for mobile phones. In *Proceedings of the 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W)* (pp. 31–32), Hong Kong, China, 27–30 June 2011.
5. Taifi, M., Shi, J. Y., & Khreishah, A. (2011). SpotMPI: A framework for auction-based HPC computing using amazon spot instances. In *Proceedings of the International Symposium on Advances of Distributed Computing and Networking (ADCN)*.
6. Popovic, O., Jovanovic, Z., Jovanovic, N., & Popovic, R. (2011) A comparison and security analysis of the cloud computing software platforms. In *Proceedings of the 2011 10th International Conference on Telecommunication in Modern Satellite Cable and Broadcasting Services (TELSIKS)* (Vol. 2, pp. 632–634), Nis, Serbia, 5–8 October 2011.
7. Gul, I., ur Rehman, A., & Islam, M. H. (2011). Cloud computing security auditing. In *Proceedings of the 2011 the 2nd International Conference on Next Generation Information Technology (ICNIT)* (pp. 143–148), Gyeongju, Korea, 21–23 June 2011.
8. Kandukuri, B. R., Paturi, V. R., & Rakshit, A. (2009). Cloud security issues. In *IEEE International Conference on Services Computing, 2009. SCC'09* (pp. 517–520).
9. Chen, Z., & Yoon, J. (2010). IT auditing to assure a secure cloud computing. In *2010 6th World Congress on Services (SERVICES-1)* (pp. 253–259).
10. Kandukuri, B. R., Paturi, V. R., & Rakshit, A. (2009). Cloud security issues. In *Proceedings of the IEEE International Conference on Services Computing, 2009 (SCC'09)* (pp. 517–520), Bangalore, India, 21–25 September 2009.
11. Chen, Z., & Yoon, J. (2010). IT auditing to assure a secure cloud computing. In *Proceedings of the 2010 6*th *World Congress on Services (SERVICES-1)* (pp. 253–259), Miami, FL, USA, 5–10 July 2010.
12. Ryan, G. W., & Bernard, H. R. (2013). *Data management and analysis methods*. Available online: http://www.rand.org/pubs/external_publications/EP20000033.html. Accessed on 25 August 2013.
13. Khalil, I., & Bagchi, S. (2011). Stealthy attacks in wireless ad hoc networks: detection and countermeasure. *IEEE Transactions on Mobile Computing, 10*(8), 1096–1112.
14. Panta, R. K., Bagchi, S., & Khalil, I. (2009). Efficient wireless reprogramming through reduced bandwidth usage and opportunistic sleeping. *Ad Hoc Networks (an Elsevier Journal), 7*(1), 42–62.
15. Almorsy, M., Grundy, J., & Müller. I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.

16. Fangfei, Z., Goel, M., Desnoyers, P., & Sundaram, R. (2011). Scheduler vulnerabilities and coordinated attacks in cloud computing. In *Proceedings of the 2011 10th IEEE International Symposium on Network Computing and Applications (NCA)* (pp. 123–130), Cambridge, MA, USA, 25–27 August 2011.
17. Karnwal, T., Sivakumar, T., & Aghila, G. (2012). A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack. In *Proceedings of the 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS)* (pp. 1–5), Bhopal, India, 1–2 March 2012.
18. Gruschka, N., Jensen, M. (2010). Attack surfaces: A taxonomy for attacks on cloud services. In *Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD)* (pp. 276–279), Miami, FL, USA, 5–10 July 2010.
19. Oberheide, J., Cooke, E., Jahanian, F., & Cloud, A. V. (2008). N-version antivirus in the network cloud. In *Proceedings of the 17th Conference on Security Symposium (SS '08)* (pp. 91–106) USENIX Association:Berkeley, CA, USA, 2008.
20. Top Threats to Cloud Computing V1.0; Cloud Security Alliance: March 2010.
21. Tupakula, U., Varadharajan, V., & Akku, N. (2011). Intrusion detection techniques for infrastructure as a service cloud. In *Proceedings of the 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC)* (pp. 744–751), Sydney, Australia, 12–14 December 2011.
22. Liu, B., Xu, E., Wang, J., Wei, Z., Xu, L., & Zhao, B. et al. (2011). Thwarting audio steganography attacks in cloud storage systems. In *Proceedings of the 2011 International Conference on Cloud and Service Computing (CSC)* (pp. 259–265), Hong Kong, China, 12–14 December 2011.
23. Szefer, J., & Lee, R. B. (2012). Architectural support for hypervisor-secure virtualization. *SIGARCH Computer Architecture News, 40,* 437–450.
24. Motawie, R., El-Khouly, M. M., & El-Seoud, S. A. (2016). Security problems in cloud computing. *International Journal of Recent Contributions from Engineering, Science & IT (iJES),* 4(4), 36–40.