SURVEY OF SECURITY CHALLENGES AND ATTACKS IN CLOUD.

Mirza Sadaf Rasool
Department of Computer Science,
Jamia Hamdard, New Delhi, India

Abstract- Cloud Computing has become the most popular technology of choice for organizations today. The on-demand, and "pay as you go" features make it even more attractive as a technological choice. Scalability and flexibility play their crucial role in many of the promising features of cloud computing. However, they may as well bring along certain challenges and limitations to it. Various security issues pertaining to the cloud service models are highly likely to induce vulnerabilities. These vulnerabilities may be exploited by malicious intruders to launch various attacks. This paper broadly discusses some of the security issues of the cloud. Few of the many possible attacks on cloud computing are have also been discussed. It also presents a review of some proposed solutions in the literature.

Keywords- *Cloud Computing, Virtual machine, Attack.*

1. INTRODUCTION

Cloud Computing is a technology which is emerging as a means for small as well as medium business companies to gain access to services such as shared resources, software, infrastructures etc. The cloud service can be availed on demand over the Internet, with very less investment in infrastructure and purchase of new software. NIST has defined cloud computing as a "model for enabling ubiquitous, 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" in [1]. Cloud services follow a "pay as you go" model, which allows it to be used as a utility, and pay only for the services used. Industries are driven to use a Cloud service due to its minimal investment, cost reduction, and rapid deployment, which allows them to concentrate on core business problems and priorities instead of having to deal with technical issues [2].

Cloud computing provides to its users services to users through different technologies like multitenancy, virtualization, and, web services [3].

Web Service: Web Applications are used to access the services over the Internet.

Virtualization: The processes and applications of users are run in a virtualized environment. The virtual environment uses physical resources.

Multitenancy: The virtual processes of different users may run on same physical resource. These processes are logically separated. It makes the cloud, a multitenant technology.

Cloud Services are provided as three distinct types: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [1], [4].

Software as a Service (SaaS): The cloud service provider hosts applications on the cloud environment. This service can be accessed via a web browser through the Internet. The users are not required to install the applications on their computers. The SaaS provider may host the applications on its own data centers or may deploy the applications on the infrastructure provided by a third party such as Amazon, Google, Microsoft etc. [5].

Platform as a Service (PaaS): PaaS provides the framework (or platform) for development and testing of applications. Developers can run develop their applications without having to download or install the required platform on their computers.

Infrastructure as a Service (IaaS): IaaS provides to the user a virtual space for storage, to deploy servers and cloud networks. IaaS provides hardware as a virtual machine for on demand services. The IaaS provider is responsible for the maintenance of the infrastructure provided, which can include Operating systems as well.

Because Cloud Services are deployed over the Internet, security of these services becomes vulnerable. Cloud environment runs on standard Internet protocols, use virtualization methods which make it a target to many types of attacks [6]. Cloud Security can become an easy target of attacks such as Denial of Service, Distributed Denial of Service, IP spoofing, etc.

The vulnerabilities of cloud computing may be further exploited to launch more advanced and complex attacks such as zombie attacks, man in the middle attack, service injection attacks, backdoor channel attacks, attack on virtualization, phishing attacks etc. [2].

The cloud services may be deployed in any of four models: Public Cloud, Private Cloud, or a Hybrid Cloud, Community Cloud [1].

The technology used, the underlying service model, and deployment model put cloud computing at a risk of threats and attacks despite of their numerous advantages. Security issues of cloud computing becomes one of the main challenges in realizing the widely accepted adoption of cloud computing [7].

2. SECURITY ISSUES IN CLOUD COMPUTING

The challenges in terms of security for cloud computing are not only tremendously large in number, but have varied level of complexities too. This section discusses few major challenges roughly based on issues in the architecture, and issues in communication.

2.1 Issues in communication

Communication on the cloud may be between the user and the cloud, or among the components of the cloud. The components of a network are shared along with the resources for storage and computation [8], which can result in a cross-tenant attack [9]. The users may be provided with super-user privileges for management of their Virtual Machines (VMs) which may allow an intruder to launch sniffing or spoofing attacks [3].

2.1.1 Security Misconfiguration

As the data and applications of the customers are present remotely on the cloud, the misconfiguration of cloud may lead to breach in the security of the hosted applications and data. It may even compromise the complete system [10].

2.1.2 Virtual Network

Security of virtual network cannot be monitored by the security measures available for the physical network [3]. Moreover, Virtual machines may share a virtual network. This can make the virtual network a target for attacks such as spoofing and DoS [3].

2.2 Issues in architecture

2.2.1 Virtualization

Different users can use the same resource due to the virtualization. However, security of the cloud infrastructure and data can be affected by virtualization. These issues are discussed under:

Virtual Machine Isolation: The virtual machines logically present on the same physical resources may cause cross Virtual Machine attacks.

Virtual Machine Image Sharing: Users are allowed to create their own virtual machine images. They are also allowed to download, or upload images [11]. The attackers may thus be able to upload an infected image.

Virtual Machine Rollback: When an image is rolled back to some previous state, it may return the Virtual machine to a former configuration error [12].

Virtual Machine Migration: During the migration of a virtual machine to another physical machine data and the code become vulnerable to attacks [3]. An attacker might migrate the virtual machine to an infected server [3].

Hypervisor Issues: An infected hypervisor can affect the security of the virtual machines under its control.

2.2.2 Storage and Data Issues

Even though the users have certain control over the virtual machine, they don’t have much control on their stored data. It results in some security issues related to the data such as:

Integrity and Privacy: Both, the data at rest and the data being processed may be at risk due to multitenancy [12]. A malevolent user may infect data of other users.

Data Backup: To recover from any accidental deletion of the data, the cloud service provider must ensure secure data backups exist.

Data Recovery: A user may be allocated a resource that was previously allocated another user. A malicious user may be able to recover deleted data from the resource allocated to him [3].

2.2.3 Access Control

The users of cloud may come from organisations with different framework for authentication and authorization [14]. Therefore cloud requires an authorization process which is dynamic and detailed in nature.

2.2.4 API and Web Application Security

Some of risks identified in [14] are: Injection, Cross Site Scripting, Broken Authentication, and Session Management, Security Misconfiguration, Invalidated redirects and forwards etc. To secure the web applications these threats must be taken into account while developing and using web applications. APIs that are published by the cloud service providers help users to know the functions and details of the cloud [3]. This exposes the architecture of cloud to attackers to certain extent [16].

3. COMMON ATTACKS IN CLOUD COMPUTING

3.1. Zombie attack

An attack on a host is done by flooding from it a large number of requests into the network. Since any one can access a Virtual Machines through the Internet, a large number of zombie attacks may be launched by the attacker causing DoS or DDoS. Zombie attacks might cause Denial of Service (DoS) if the attack compromises the specific service provided by a server [2], [6]. In case a server provides multiple services, and all of those are denied due to the attack, it may cause Distributed Denial of Service (DDoS) [2], [6].

3.2. Man in the Middle Attack

An attacker tries to sniff the information exchanged between the communicating parties. The attacker sits in the middle of the logical communication path. The attacker appears as legitimate receiver to the sender, and a legitimate sender to the original sender. Such attacks may be a result of the vulnerabilities in the underlying authentication network protocols such as SSL. Since the authentication is usually provided by third parties, so the certificate generation system itself may become a cause of this attack [17].

3.3. Cloud Malware Injection Attacks

It is an attack on the Services, or the Virtual Machine itself. An attacker may create an illegitimate instance of a service (SaaS, Paas, or IaaS) provided, or an instance of the Virtual Machine. When such an instance is run on the cloud, the users are provided with malicious services. The situation can worsen if an attacker is successful in executing a malware on the cloud. The Cloud treats the malware as a valid instance [18]. This malware may affect the underlying hardware, and thus other services that run on the hardware.

3.4. Backdoor Channel Attacks

This is a passive attack that compromises confidentiality of the user. The attacker is able to gain access to the affected node remotely, and thus gain access to the confidential data of users. Once an attacker has gained access, it can make the affected resources into zombies. The zombies can be further used to cause DoS or DDoS attacks [19].

3.5. Attack on Virtualization

The attack compromises the hypervisor, thus affecting the related virtual machines. The attack can be either a VM Escape, or Rootkit in Hypervisor [2], [20].

VM Escape: This attack causes an attacker's program to gain hypervisor root privileges [2]. The attacker can communicate with the hypervisor directly, and as a result affect other virtual machines

Roorkit Hypervisor: It compromises the Operating System, a guest operating system acts as a host Operating System [2]. The new host OS gains access to the underlying resources.

3.6. Phishing Attack

An unauthentic link is forwarded to the victim users. This link looks legitimate but redirects the users to malicious websites. This type of attack can cause breach in sensitive information of users. The attacker may be able to host a manipulated site on the cloud service, and gain unauthorized access to user's accounts [21].

4. REVIEW OF LITERATURE

In this section we mention some approaches suggested in literature for cloud security, and detection of attacks.

Xiangjian He, et al. (2013) in [22] propose a novel model of firewall called "Tree-Rule Firewall". This paper describes that the Listed-rule firewalls faced security, difficult to use, and speed issues due to their limitations. Shadowed rule, redundant rule, and sequential rule lead to degraded security. Moreover, using bigger rules after small rules cause difficult to use issues, and redundant rules cause decreased speed. Tree-rule firewall is free from all these issues. The conventional Listed-rule firewall presents rules as a list of rules, while as in the tree-rule firewall it proposed to present the in a tree from. The suggested firewall reads the first attribute from the packet header and compares it with the information at the root node. Then successive attributes are read and compared with the next level of tree in order. This results in a faster decision on the packets. Moreover, Tree-rule firewall is easier to design than the Listed-rule firewall.

Kazim, M., et al. (2013) in [23] describe securing of virtual disc images by proposed novel model called "Encrypted Virtual Disc Images in Cloud (EVDIC)". It also describes the integration of EVDIC with OpenStack. EVDIC encrypts the virtual disc images using AES-256 before storing them. After the VM images have been encrypted they are stored on the cloud.

Encryption of the virtual disc image prevents it from unauthorized access, malwares, and ensures data integrity. To launch a virtual machine, the stored encrypted VM image is identified and decrypted. This encryption-decryption model ensures the integrity and confidentiality of the data.

Sushmita Ruj, et al. (2014) in [24] propose a novel scheme for access control. This scheme is decentralized and provides data access to only users with valid attributes. The proposed method presents an anonymous authentication of the users, but provides authentication of users who modify and store data on the cloud. The proposed method ensures that the revoked users are not able to access the data after their revocation. The scheme ensures prevention of replay attacks.

Hashim A., et al. (2014) propose in [25] an integrated Intrusion Detection System (IDS). The authors propose integrating a Hidden Markov Model (HMM) with the Autonomous Cloud Intrusion Detection Framework (ACIDF). The ACIDF collects information from various sensors and produces normalized events. It then assesses the risk, which is then followed by prediction of attacks by the HMM. The sequence of transitions in this HMM represents the sequence of events in an attack signature and the output on transition depends on the event. The output of the HMM represents an attack state. Following it, an approached based on the fuzzy logic is employed for a correct response. If the probability predicted exceeds a threshold, then an alarm is generated.

Kushwah, et al. (2017) propose a model for detection of DDoS in [26]. The model uses Black Hole optimization algorithm [27] in the training process. It produces a set of solutions. These solutions determine the weights for the Artificial Neural Network (ANN). The model uses ANN for classification. The weight vectors are used to evaluate an objective function. The objective function in this case is to minimize the Minimum Squared Error.

Xin Liang, et al. (2017) propose in [28], a novel approach for placement of Virtual Machine (VM). The approach is grouping-based, and provides an optimization of the existing policy for placement of the VM. The approach is secure one, and promises substantial decrease in the probability of co-resident attack. The placement of VM is done by group selection and host selection. The suggested approach divides all the available physical severs into number of groups. This is done by following some grouping strategy such as a simple random technique or a round robin technique. Followed by the grouping, a physical server is selected from the selected group. This physical server serves as a host for the VM. The group selection ensures secure optimization, and the host selection ensures the resource optimization. Although there is a little decrease in the resource efficiency, it is a trade-off with the co-location resistance.

Chouhan M., et al. (2015) in [29] propose a novel approach to detect Cache-based Side Channel Attack (CSCA). The proposed approach uses a Blooming Filter (BF), which makes the detection of CSCA more effective and flexible. The approach uses a timer to record the Cache Miss Time (CMT). It then finds the Cache Miss Sequence (CMS) by arranging the CMT in ascending order. The mean between the difference of each consecutive CMT is calculated and a hash function is applied to it. The hash value is then supplied to the BF. BF stores the CMS values during previous CSCA. A set membership task is carried by the BF on receiving the hash value. This results in a decision to either wait for a context switch, or to execute a mechanism for prevention. If the value of set membership was true, then there are very high chances of a CSCA. In this case a prevention mechanism is followed. Otherwise, the system waits for a context switch. The proposed solution promises to be adaptive, and detects novel CSCA techniques.

5. CONCLUSION

In this paper an overview of cloud computing has been presented. Also, various security issues of cloud, along with some of the possible attacks on cloud computing have been discussed. Furthermore, review of existing techniques has been given through a literature survey. It has been found that with increased demand for cloud computing, the nature and types of attacks are increasing both in complexity and number respectively. To handle these attacks and security issues, approaches based on IDS as well as algorithmic approaches have been suggested in existing literatures. Few of these approaches have been discussed in this paper.

ACKNOWLEDGEMENTS

I would like to thank my supervisor Prof. Ranjit Biswas for his constant support.

REFERENCES

1. P. Mell, T. Grance, *The NIST Definition of Cloud Computing*, US National Institute of Science and Techonology Std., 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

2. C., Modi,, D., Patel, et al., "A survey on security issues and solutions at different layers of Cloud computing", *The Journal of Supercomputing*, vol. 63, pp. 561, 2012.

3. M., Ali, S.U. Khan, et al., “Security in cloud computing: Opportunities and challenges,” *Information Sciences*, 2015, vol. 305, pp. 357-383.

4. F. Luo, Z. Y. Dong., et al., “Hybrid cloud computing platform: The next generation IT backbone for smart grid,” in *Proc. Of IEEE Conf. on PES General Meeting*, pp. 1–7, 2012.

5. S.Subashini, V.Kavitha, “A survey on security issues in service delivery models of cloud computing”, *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1-11, 2011.

6. C., Modi, D., Patel, et al., “A Survey of Intrusion Detection Techniques in Cloud”, *Journal of Network and Computer Applications*, vol. 36, pp. 42-57, 2013.

7. R. Latif, H. Abbas, et al., “Cloud Computing Risk Assessment: A Systematic Literature Review,” *In Future Information Technology, Springer Berlin Heidelberg*, 2014, pp. 285-295.

8. D. AB. Fernandes, L. FB Soares, et al., “Security issues in cloud environments: a survey,” *International Journal of Information Security*, vol. 13, no. 2, 2014, pp. 113-170.

9. K. Hashizume, D. G. Rosado, et al., “An analysis of security issues for cloud computing,” *Journal of Internet Services and Applications*, vol. 4, no. 1, 2013, pp. 1-13.

10. A. Eghtesadi, Y. Jarraya, et al., “Preservation of Security Configurations in the Cloud,” *In IEEE International Conference on Cloud Engineering (IC2E)*, 2014, pp. 17-26.

11. W. A. Jansen, “Cloud hooks: Security and privacy issues in cloud computing,” *In 44th Hawaii International Conference on System Sciences (HICSS)*, 2011, pp. 1-10.

12. K. Hashizume, D. G. Rosado, et al., “An analysis of security issues for cloud computing,” *Journal of Internet Services and Applications*, vol. 4, no. 1, 2013, pp. 1-13.

13. M. Sookhak, H. Talebian, et al., “A review on remote data auditing in single cloud server: Taxonomy and open issues,” *Journal of Network and Computer Applications*, vol. 43, 2014, pp. 121-141.

14. B. Liu, E. Blasch, et al., “Information Fusion in a Cloud Computing Era: A Systems-Level Perspective,” *IEEE Aerospace and Electronic Systems Magazine*, vol. 29, no. 10, 2014, pp. 16-24.

15. Open Web Application Security Project Top 10-2013, “The ten most critical Web application security risks,” https://www.owasp.org/index.php/Top10]OWASP Top 10 for 2013 [accessed on: April 08, 2014]

16. H. Yu, N. Powell, et al., “Cloud computing and security challenges,” *In Proceedings of the 50th Annual Southeast Regional Conference, ACM*, 2012, pp. 298-302.

17. Subodh, G., “A Review of Man-in-the-Middle Attacks,” eprint arXiv:1504.02115, 2015.

18. N. Gruschka, M. Jensen, “Attack Surfaces: A Taxonomy for Attacks on Cloud Services,” *2010 IEEE 3rd International Conference on Cloud Computing*, Miami, FL, 2010, pp. 276-279.

19. Z. Chiba, N. Abghour, et al., “A survey of intrusion detection systems for cloud computing environment,” *2016 International Conference on Engineering & MIS (ICEMIS)*, Agadir, 2016, pp. 1-13

20. Munir, Kashif et al., “Secure Cloud Architecture”, *Advanced Computing: An International Journal*, vol. 4, pp. 9-22, 2013

21. Shilpa, D., Nagashree, C. et al., “Survey on Security Attacks and Solutions in Cloud Infrastructure”, *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3, no. 8, pp. 7757-7761

22. He, X., Chomsiri, T. et al., “Improving cloud network security using Tree-Rule firewall”, *Future Generation Computer Systems* (2013), http://dx.doi.org/10.1016/j.future.2013.06.024

23. Kazim, M., Masood, R. et al. “Securing the virtual machine images in cloud computing”, In *Proceedings of the ACM 6th International Conference on Security of Info and Networks*, pp. 425-428, 2013.

24. S. Ruj, M. Stojmenovic, et al., “Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds,” in *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 384-394, Feb. 2014.

25. H. A. Kholidy, A. Erradi, et al., “A Finite State Hidden Markov Model for Predicting Multistage Attacks in Cloud Systems,” *2014 IEEE 12th International Conference on Dependable, Autonomic and Secure Computing*, Dalian, 2014, pp. 14-19.

26. G. S. Kushwah and S. T. Ali, “Detecting DdoS attacks in cloud computing using ANN and black hole optimization,” *2017 2nd International Conference on Telecommunication and Networks (TEL-NET)*, Noida, India, 2017, pp. 1-5.

27. A. Hatamlou, “Black hole: A new heuristic optimization approach for data clustering”, *Information sciences*, vol. 222, 2013, pp. 175-184.

28. X. Liang, X. Gui, et al., "Mitigating cloud co-resident attacks via grouping-based virtual machine placement strategy," *2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC)*, San Diego, CA, 2017, pp. 1-8.

29. M. Chouhan and H. Hasbullah, "Adaptive detection technique for Cache-based Side Channel Attack using Bloom Filter for secure cloud," *2016 3rd International Conference on Computer and Information Sciences (ICCOINS)*, Kuala Lumpur, 2016, pp. 293-297.