A Review on Security Issues in Cloud Computing

[1]Satinder Kaur, [2]Dr. S S Khurmi
[1]Asst. Prof in Computer Applications Dept., SGGSWU, Shri Fatehgarh Sahib, Punjab, India
[2]Professor, Dept. of Computer Sciences, Desh Bhagat University, Mandi Gobindgarh, Punjab, India

Abstract
Security is the one of the major issues today in network applications around the world. In other words Security is the barrier for the adoption of Cloud Computing. In this paper, we will highlight the major security threats in Cloud Computing Systems and also discuss about the different aspects to be focused while talking about cloud security. We have categorised these threats from different viewpoint, providing a helpful and little-known list of threats. After that some effective counter measures area are listed and explained.

Keywords
Security Issues, Cloud Computing, Threats, Countermeasures

I. Introduction

Cloud Computing is on-demand service model for IT provision often based on virtualization and distributed computing technologies. It delivers applications and storage spaces as services over the internet. As a result, all the major companies including Microsoft, Google and Amazon are using cloud computing. There is no doubt that the convenience and low cost of cloud computing services have changed our daily lives. However, security issues associated with cloud computing make us vulnerable to cybercrime that happen every day. The CSA guide presents the security threats for cloud. However, in order to control and avoid these threats there is needs for survey. In this paper we define these threats, which are possible to exploit and their effects on cloud entities.

II. Security Threats in Cloud Computing

Cloud Computing is an emerging technology with shared resources and lower cost that relies on pay per use according to the users' demand. Due to its characteristics, user may face lots of threats and problems. In this section the major threats for cloud computing are explored.

A. Threats to cloud computing discovered by "Cloud Security Alliance" (CSA):

CSA is a renowned community in the scope of cloud security. The threats are as follows:

1. Abuse and Nefarious use of Cloud Computing

Abuse and Nefarious use of cloud computing is the top most threat identified by CSA. Attackers can infiltrate a public cloud, for example, they find a way to upload malware to thousands of computers.

2. Insecure Interfaces and API

Application Programming Interface (API) is a set of protocols and standards that define the communication between software applications through internet. The security of various cloud services depends on the APIs security. Cloud providers generally offer their APIs to third party to give service to customers. However, weak APIs can lead to the third party having access to the critical information in cloud.

3. Malicious Insiders

The threat of a malicious insider is well-known to most organizations. They have access to most data and resources, and might end up using their access to leak that data.

4. Shared Technology issues

Cloud Computing provide services on shared basis such as PaaS, IaaS, SaaS. However different components such as CPU, GPU etc may not offer cloud security requirements. In recent years, shared technology issues have been used by attackers to attack on cloud, how to impact operations of other cloud customers and how to gain unauthorized access to data.

5. Data Loss or Leakage

Data loss or leakage is most sensitive matter for any organization. Data loss mostly occurs due to malicious attackers, data deletion, data corruption, loss of data encryption keys or natural disasters.

6. Account or Service Hijacking

Account or Service Hijacking is not new. It involves the stealing of user credentials to get access to his account, data or other information.

B. Security Threats related to the location of the Cloud System:

In Cloud Computing systems, data storage is spread around the world. This may lead to some security problems that are as given below:

1. Multi-location of the Private Data

In Cloud Computing the private data is/are placed in someone else's computer. There many things can go wrong. Firstly, the Cloud service provider may go out of business. Secondly, the cloud service provider may decide to hold the data as hostage if there is a dispute. Thirdly, it is rather important for a company to understand in which country its data will be hosted.

2. Data Combinations

The cloud Computing client needs to ensure that its private data is stored separately from others or not. If they are combined with those of other clients' data then it is much more dangerous.

3. Data Location

It might be rather difficult or even impossible for the cloud service provider to assure the locations where the client's data will be stored.

4. Data Transfer Across the Borders

Knowing where the cloud service provider will host the data is a prerequisite to know how to transfer data across the country borders, which makes the law to be applied even more complicated and consequently resulting in the private information to be more vulnerable from attack.

C. Security Threats inherited from Network Concept

Network plays an important role in deciding how efficiently the cloud services operate and communicate with user. The most critical network threats in Cloud are listed below:-

1. SQL Injection Attacks

In this type of attack a malicious code is inserted into a standard SQL code. Thus the attacker gain unauthorized access to a database and are able to access sensitive data.

2. Man in the Middle Attacks

In this type of attack, an entity tries to intrude in an ongoing conversation between a sender and a client to inject false information and to have knowledge of the important data transferred between them.

3. Security Concerns with the Hypervisor

Cloud Computing rests mainly on the concept of virtualization. In a virtualized world, hypervisor is defined as a controller popularly known as virtual machine manager (VMM) that allows multiple operating systems to be run on a system at a time. Since multiple operating systems would be running on a single hardware platform, it is not possible to keep track of all such systems and hence maintaining the security of the operating systems is difficult.

4. Denial of Service Attack

DoS (Denial of Service Attack) are done to prevent the authorized from accessing cloud services.

5. Distributed Denial of Services Attacks

Distributed Denial of Services Attacks (DDoS) attack is a form of DoS attacks in which multiple network sources are used by the attacker to send a large number of requests to the cloud for consuming its resources.

III. Security Countermeasure in Cloud Computing

In this section the security methods to avoid the exploitation of threats mentioned in section II.

A. Countermeasure for CSA Threats

There are also some threats, stated by Cloud Security Alliance. There are some counter measures to confront these threats. These are as follows:

1. Abuse and Nefarious use of Cloud Computing

To avoid this threat, enhance credit card fraud monitoring and coordination, and Comprehensive introspection of customer network traffic.

2. Insecure Interfaces and API

To protect the cloud from insecure API threats cloud provider must ensure that all the APIs implemented in cloud are designed securely. Strong authentication mechanisms and access controls must also be implemented to secure data and services from insecure interfaces and APIs.

3. Malicious Insiders

To avoid this threat, there is need to specify human resource requirement as part of legal contracts, and require transparency into overall information. Another method is by limiting the hardware and infrastructure access only to the authorized personnel. Strict action should be taken against malicious activities.

4. Shared Technology issues

To confront this threat, there is need to monitor environment for unauthorized activity and promote strong authentication and access control.

5. Data loss/leakage

To prevent data loss in cloud, different security measures can be adopted. One of the most important measures is maintain backup of all data in cloud. Another method is to implement strong API access control.

6. Account or Service Hijacking

Account or service hijacking can be avoided by adopting different security features on cloud network. These include employing Intrusion Detection Systems (IDS) in cloud to monitor network traffic and nodes for detecting malicious activities.

B. Countermeasure for Security Threats inherited from Network Concept

In order to avoid Security Threats inherited from Network Concept are as given below:

1. SQL Injection Attacks

A proxy based architecture is used towards preventing SQL injection attacks.

2. Man in the Middle Attacks

A few might be considered in order to avoid this threats are: software as a service, separate endpoint and server security process, evaluating virtualization at the end point have been done to tackle with this kind of attack in cloud computing.

3. Security Concerns with the Hypervisor

Security concerns with the hypervisor can be avoided is to develop advanced cloud protection system by monitoring the activities of the guest VMs (virtual machines) and inter-communication among the various infrastructure components.

4. Denial of Service Attacks

Usage of an Intrusion Detection System (IDS) is the most popular method of defence against this type of attacks.

5. Distributed Denial of Service Attacks

The use of IDS in the virtual machine is used to protect the cloud from DDOS attacks. Another method commonly used to guard against DDOS is to have intrusion detection system on all physical machines.

IV. Conclusion

Cloud Computing is one of the most significant shifts in information and technology. However, there are different Security issues associated with it. In order to obtain user confidence, security should be considered as an important part of cloud. In this paper we discuss about various security threats and impact of these threats on cloud user and provider. We have also provide some effective counter measures to avoid security threats in cloud computing.

References

[1] Weichao Wang, Zhiwei Li, Rodney Owens, Bharat Bhargava. "Secure and Efficient Access to Outsourced Data", CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security, pp. 55-65. November 2009.

[2] Claudio Mazzariello, Roberto Bifulco and Roberto Canonico, "Integrating a Network IDS into an Open Source Cloud Computing Environment", Sixth International Conference on Information Assurance and Security, USA, pp. 265-270, Aug. 23-25, 2010.
[3] K. Vieira, A. Schulter, C. B. Westphall, C. M. Westphall, "Intrusion detection techniques for Grid and Cloud Computing Environment", IT Professional, IEEE Computer Society, Vol. 12, Issue 4, pp. 38-43, 2010.
[4] Ruiping Lua and Kin Choong Yow, "Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network", IEEE Network, Vol. 25, No. 4, pp. 28-33, July-August, 2011.
[5] Flavio Lombardi, Roberto Di Pietro, "Secure Virtualization for Cloud Computing", Journal of Network and Computer Applications, Vol. 34, Issue 4, pp. 1113- 1122, July 2011, Academic Press Ltd. London, UK.
[6] Hanqian Wu, Yi Ding, Winer, C., Li Yao, "Network Security for Virtual Machines in Cloud Computing", 5th Int'l Conference on Computer Sciences and Convergence Information Technology, pp. 18-21, Seoul, Nov. 30-Dec. 2, 2010
[7] A. Liu, Y. Yuan, A Stavrou, "SQLProb: A Proxybased Architecture towards Preventing SQL Injection Attacks", SAC March 8-12, 2009
[8] Gurdev Singh, Amit Sharma, Manpreet Singh Lehal, "Security Apprehensions in Different Regions of Cloud Captious Grounds", International Journal of Network Security & Its Applications (IJNSA), Vol. 3, No. 4, July 2011.
[9] Shengmei Luo, Zhaoji Lin, Xiaohua Chen, Zhuolin Yang, Jianyong Chen, "Virtualization security for cloud computing services", Int. Conf on Cloud and Service Computing, pp. 174-179, Dec, 2011.
[10] T. T. W. Group et al., "The notorious nine: cloud computing top threats in 2013," Cloud Security Alliance, 2013.
[11] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan,"A survey of intrusion detection techniques in cloud," Journal of Network and Computer Applications, Vol. 36, No. 1, pp. 42–57, 2013.
[12] Kazim.M, and Zhu S.H,"A survey on top security threats in cloud computing",International Journal of Advanced Computer Science and Applications,vol. 6, no.3, pp.109-113,2015.
[13] Ashktorab,Taghizadeh,"Security Threats and Counter-measures in Cloud Computing", International Journal of Application or Innovation in Engineering & Management, Vol. 1, Issue 2, pp. 234-245, 2012.

Satinder Kaur is a Ph.D. Candidate under the guidance of Dr. Sawtantar Singh Khurmi at Desh Bhagat University; Mandi Gobindgarh.She did Masters of Computer Applications (MCA) from Punjabi University, Patiala .Currently she is working as Assistant Professor in Sri Guru Granth Sahib World University, Fatehgarh Sahib. Her area of research is Cloud Computing, Service Level Agreement and Security issues.