ISSN No. 0976-5697

Volume 5, No. 5, May-June 2014

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Survey on Cloud Computing

Chander Diwaker
University Institute of Engineering and Technology
Kurukshetra University
Kurukshetra, India

Priyanka Dembla
University Institute of Engineering and Technology
Kurukshetra University
Kurukshetra, India

Abstract: Cloud is an emerging computing technology in which resources and services of computing infrastructure are provided as services over the Internet - namely, the hardware and systems software in data centers that provide these services. It is a network-based environment that gives importance on sharing computations or resources. Many enterprises are dependent on cloud providers for their services and resources. This dependency can cause huge problem if it is attacked by an attacker. Thus security is one of the major challenges for cloud service providers and consumers**.**

Keywords: Cloud, Security, Attacks, Issues

I. INTRODUCTION

Cloud computing is one of the most hyped information technology and it has become one of the fastest growing segments of IT. Costumers must only pay for the amount they are using and have not to pay for local resources such as storage or infrastructure. The cloud offers several benefits like fast deployment, pay-for- use, lower costs, scalability and flexibility. Resources such as hardware and software are liable to be outdated soon. Therefore outsourcing of resources is the solution.

II. SERVICE MODELS

A. Software as a Service(SAAS):

Users have to install software application on their hard disk before using it. However in cloud computing, service providers enable and provide applications software as on demand services. Cloud users do not have to purchase software rather the payment will be based on Pay-Per-Use model. Examples of the providers are NetSuite, Oracle, IBM and Microsoft, Google Apps.

B. Platform as a Service(PAAS):

In PAAS, development environment is provided as a service to the customers. Vendor's block of code is provided by the developers to customers for creating their own applications. Customers do not have the burden of buying and installing software or hardware required for it. They simply build its application on top of the platform provided. Examples of the providers are GAE, Microsoft's Azure.

C. Infrastructure as a Service(IAAS):

IAAS provides the infrastructure as a service to its customers. The client need not purchase the required servers, data center or the network resources. Customers can achieve a much faster service delivery with less cost. Examples of the provider are GoGrid, Flexiscale, Layered Technologies, Joyent and Mosso/Rackspace.

III. DEPLOYMENT MODEL

A. Public:

A public cloud is standard model in which providers provide several resources available to the public such as applications and storage. Users pay only for the time duration they uses the service, i.e., pay-per-use. However public clouds are less secure compared to other cloud models as all the applications and data on the public cloud are more prone to malicious attacks.

B. Private:

Private Cloud refers to internal services of a business that is not available for ordinary people. Private clouds provide services to particular group of people behind a firewall [3]. The main advantage here is that it is easier to manage security, maintenance and upgrades and also provides more control over the deployment and use as resources and applications are managed by the organization itself.

Figure 1. Types of Cloud

C. Community:

In this type of cloud deployment model, the infrastructure of the cloud is shared by limited number of people or organizations. Communities have similar cloud requirement. Community users are also considered as trusted by the organizations that are part of the community. It can be governed by a third party service provider. [4]

D. Hybrid:

Hybrid clouds are a combination of public, private, and community clouds. Hybrid clouds have advantages of each cloud deployment model. Organization manages some resources for internal use and provides other externally. Each part of a hybrid cloud is connected to the other by a gateway that controls application and data flow.

IV. ATTACKS IN CLOUDS

Due to distributed nature of cloud computing it is vulnerable to various attacks. Intruder can internally or externally attack clouds. Researchers are devoting their time in finding effective measures of preventing attacks. Some of the attacks in clouds are:

A. Cloud Malware Injection Attack:

In cloud malware injection attack, attacker changes the functionality of data or even blocks it. Attacker injects malicious service or virtual machine into the cloud. It creates its own service implementation model in case of SAAS and PAAS or virtual machine instance in case of IAAS and adds it in the cloud system.

B. Metadata Spoofing Attack:

In metadata spoofing attack, attacker maliciously redesigns a Web Service's metadata descriptions. For instance it can modify functioning of operations. So if a user calls some operation, it will look like a call to another operation.

C. IP Preffix Hijacking:

During the IP prefix hijacking attack, an attacker announces the IP prefix which belongs to the victim network. This wrong hijacking route propagates on the Internet and the nodes who choose to believe the forged route become infectors [6].

D. DDOS:

DDOS makes services or resources unavailable for indefinite amount of time for legitimate users. The attacker usually spoofs IP address section of a packet header in order to hide their identity from their victim. Various resources such as bandwidth, memory and computing power of server gets wasted in serving flooding packet [7].

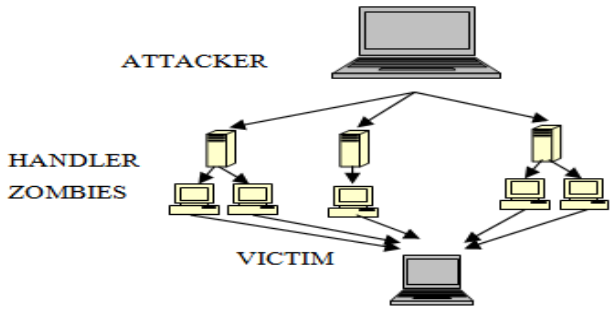

Figure 2. Components of DDOS

E. Man in the Middle Cryptographic Attack:

In this attack, an attacker inserts himself between communication path of two users and have the possibility that it can intercept and modify communication data. The attacker on behalf of the customer authenticates itself to verifier and verifier to the customer.

F. Authentication Attack:

Attacks against authentication in cloud computing is mostly targeted. Users can be authenticated in many different ways. Many organizations only uses username and password as a authentication but some financial institutes uses secondary authentication such as virtual keyboards, shared secret question etc. to prevent authentication attacks[5].

G. Masquerade Attack:

A masquerade attack is an attack in which attacker poses as, or assumes the identity of another legal user to illegally use resources. It only requires the knowledge of a person's password. Security technologies such as firewalls or authentication protocols are of no use because, after logging as a legal user, an attacker can exploit any user privilege [9].

H. EDOS:

EDOS attack is the new breed of attack. While DDOS attacks on server and network resources, it targets the cloud adopter's economic resources and is referred to as Economic Denial of Sustainability (EDoS) attack. In other words, the attack makes the cloud unsustainable by fading the cloud billing mechanism to charge the cloud user's bill for the attack's activities [10].

V. ISSUES

Although cloud computing is associated with numerous benefits but it is associated with many security risks. The challenges faced by the clouds are described below.

A. Data Loss:

When any application is running on a server, backup routine is configured so that it is safe in the event of a data-loss or disaster incident. The data should be backuped to any portable media on a regular basis which could be stored in an off-site location.

B. Integrity:

Data in the cloud should be as it is stored by the data owner. It should not be modified by any authorized person.

C. Availability:

It ensures that cloud's resources and services are not made unavailable by malicious action. It is the simple idea that when a user tries to access something, it is available to be accessed.

D. Confidentiality:

Data is not disclosed to any unauthorized persons. Confidentiality loss occurs when data can be viewed or read by any individuals who are unauthorized to access it.

E. Data Backup:

Data stored in the cloud can be changed or lost by the malicious attackers or any accidental deletion by service provider or by disaster such as earthquake, flood. This may led to permanent loss of data so proper measures should be taken such as data backup.

F. Legal Issues:

Legal issues such as Regulatory requirement, privacy laws, data security that clouds systems need to adhere [2].

But major problem is that different countries have different laws and user does not control the location where its data will be stored.

VI. LITERATURE REVIEW

Sabahi [1] explained overall security threats and responses of cloud computing. Issues such as information security policy and cloud RAS issues are also discussed in this paper. These issues are the main reasons that cause many organizations to store sensitive data in their local machines and less important ones in cloud. Author also discussed counter measures and responses which included partitioning, migration and workload analysis and allocation methods. API.Singh and Shrivastava [5] addressed different types of attacks in cloud computing environment with proper explanations and method to prevent them from attacking such as Denial of service attack, authentication attack, and side channel attacks. Cloud wars are also discussed in this paper. Cloud war is there when attacker uses a cloud for sending his flooding messages. Huang and Yang [11] presented combination of cloud computing and network security to research "cloud" firewall technology. New concepts of network security are showed including their advantages, possible risks and development trends. Cloud firewall is compared with the ordinary firewall. Jing and Jian-jun [12] surveyed the security problem of current cloud computing. A Security model is proposed based on the architecture of cloud computing. Security access control service (SACS) model has access authorization and security.

VII. CONCLUSION

Despite the potential benefits gained from the cloud computing, the organizations are not accepting it because of the security issues and challenges of clouds. They are not comfortable in storing their important data on internet where if proper precautions are not taken, can be seen by anyone. There are many attacks which hinder normal functioning of cloud. These can vary from gaining access to confidential data of user or making cloud services unavailable to legitimate users.

VIII. REFERENCES

[1] Farzad Sabahi, "Cloud Computing Security Threats and Responses", IEEE 3rd International Conference Comunication Software and Networks,2011, pp.245-249.

[2] Ziyuan, Wang, "Security and privacy issues within Cloud Computing", International Conference on Computational and Information Sciences, IEEE 2011,pp.175-178

[3] Siani Pearson and Azzedine Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing", 2nd IEEE International Conference on Cloud Computing Technology and Science, IEEE 2010, pp. 693-702

[4] Dr.Ir.W.Pieters, Prof Dr. P.H. Hartel, "Cloud Computing and Confidentiality" Master of Science graduation Thesis Computer Science - Guido Kok, May 2010.

[5] Ajey Singh, Dr. Maneesh Shrivastava, "Overview of Attacks on Cloud Computing", International Journal of Engineering and Innovative Technology, Vol.1, Issue 4,2012**,** pp.321-323

[6] Yujing Liux, Wei Peng, Jinshu Su, "Study on IP Prefix Hijacking in Cloud Computing Networks Based on Attack Planning", 10th International Conference on Trust, Security and Privacy in computing and Communication, IEEE 2011, pp.992-926

[7] Bansidhar Joshi, A. Santhana Vijayan, Bineet Kumar Joshi , "Securing Cloud Computing Environment Against DDos Attacks" 2012 International Conference on Computer communication & Informatics (ICCCI-2012) ,jan-2012, pp.1-5

[8] Examining Different Types of Intrusion Detection Systems,http://www.dummies.com/howto/content/examining-different-types-of-intrusion-detection-s.html

[9] Hisham A. Kholidy, Fabrizio Baiardi, "CIDD: A Cloud Intrusion Detection Dataset for Cloud Computing and Masquerade Attacks", in Ninth International Conference on Information Technology – New Generation, IEEE 2012, pp.397-402

[10] Madarapu Naresh Kumar, P Sujatha, Vamshi Kalva, Rohit Nagori, Anil Kumar Katukojwala and Mukesh kumar, "Mitigating Economic Denial of Sustainability (EDoS) in Cloud Computing using In-Cloud Scrubber Service" 2012 Fourth International Conference on Computational Intelligence and Communication Networks, 2012 IEEE, pp .535-539.

[11] Weili Huang and Jian Yang, "New Network Security Based On Cloud Computing" 2010 Second International Workshop on Education Technology and Computer Science, IEEE-2010, pp.604-609.

[12] Xue Jing and Zhang Jian-jun, "A Brief Survey on the Security Model of Cloud Computing" 2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science, IEEE 2010 ,pp.475-478.