Security Issues in Cloud Computing

Dhruv Haribhakti, Shreyas Loya
BTech student
ECE with specialization in IoT and sensors
VIT, Vellore, India
loyashreyas.rajesh2016@vitstudent.ac.in,
dhruv.haribhakti2016@vitstudent.ac.in

Sujatha R
Assistant Professor
Electronics department, SENSE school
VIT, Vellore, India
sujatha.r@vit.ac.in

Abstract— Cloud computing environment is a new way in which web-based applications provide a service for their users at very low computational costs through the internet. As we store data, the cloud also provides services in distributed environments. The cloud eases its users by providing virtualization technology of resources through the internet. Cloud computing is an emerging field and due to this reason, various new techniques are still developing. Hence, currently new security challenges have increased exponentially for cloud professionals. Due to the lack of security in cloud computing environment users have lost their trust in the cloud environment. Multi-tenancy, elasticity, security performance and optimization, etc. are various security issues that we face in cloud computing. In this paper we will discuss some of these issues. This paper also discusses some of the existing security technique for securing a cloud and helps researchers and professionals to know about the various security threats.

Keywords- Cloud Computing, Security Issues, Security Techniques. Data Security, Multi-Tenancy

I. INTRODUCTION

Computing undergoes many changes through grid computing to cloud computing. A new computing model proposed by the researchers in computer industry is known as “cloud computing” [1], which commercializes its previous models [2]. Cloud computing environment, is a major achievement in computing, which can bring reforms in the IT industry. This makes the IT industry more attractive and useful to the users and creates the way to designs and purchases in the IT industry [3]. It would also be changing people’s livelihood and work style. One of the definitions of Cloud computing is “a mix approach of grid and utility computing which together form a collection of dynamically interconnected computers”. It is presented as a more unified computing resource which is built on service-level agreements (SLAs).

As cloud computing is still a new and evolving field it provides a new technology for industries. PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) types of applications are defined in cloud computing. Platform as a service provides server configuration and reconfiguration. Physical/virtual machine is use as a server. On the other side, cloud computing described applications are accessible via internet and for this reason huge data centers and powerful servers are required. Major difference between Cloud computing and traditional computing are their varying properties such as their elasticity, scalability ease of resources. They also provide various levels of services to their users.

The paper concentrates on study of cloud computing with several security risks, and their corresponding counter measures.

The rest of the paper is organized as follows:

Section II Cloud service Model. Section III Cloud deployment model. Section IV Cloud security issues. Section V Technique to secure data in cloud computing. Section VI. Risks and security consideration. Finally, the paper was concluded in section VII

II. CLOUD SERVICE MODELS

A. Software as a Service

Software as a Service sometime referred as “on-demand”, is software delivered model in which user can individually provision its resources as requirement without any interaction with cloud service provider. SaaS is typically accessed by customer using a web browser. Saas application are often updated more frequently as compare with traditional software. SaaS has become delivery model for various business applications, likes Payroll Processing, CRM (Customer Relationship management), MIS (Management information System), ERP (Enterprise resource planning) and HRM (Human Resource management and Service).

B. Platform as a Service

It provides a computing platform and a solution stack as a service. In this service model, the costumer creates the software using tools and libraries from the provider. The service delivery model also provides virtualized servers and associated services for running existing application. The provider provides the server, hardware, storage and networking. The main advantage of PaaS that it allows higher level programming and multiple developers are work simultaneously on a single project.

C. Infrastructure as a Service

It provides virtualized computing resources over internet and also provide capability to the consumer by which, it can provision processing, storage, hardware, servers and network and other fundamental computing resources where the consumers can deploy and run the software (i.e. operating systems and applications).

III. CLOUD DEPLOYMENT MODEL

A. Public Cloud

It is the computing model based on the standard computing model in which utility computing is available to the general public over internet in payment bases. The main benefits are scalability, resources are properly utilized and inexpensive.

B. Private Cloud

This type of the cloud is dedicated to a single organization. It also provides scalability and self-service.

C. Community Cloud

Community cloud is a multi-tenant infrastructure. In which, the infrastructure of the cloud is shared among several organizations and supports a specific community with common computing concerns.

D. Community Cloud

The cloud infrastructure that is a composition of at least one public and one private cloud.

IV. EXISTING SECURITY THREATS

Above models and services have various cloud security issue. In most applications, confidential data is stored at servers. Securing data is always vital importance. So many challenges regarding security. Leakage of confidential data fatal many computing systems today. For example, last year marks a peak in data breaches about 740 million records were exposed, the largest number till now.

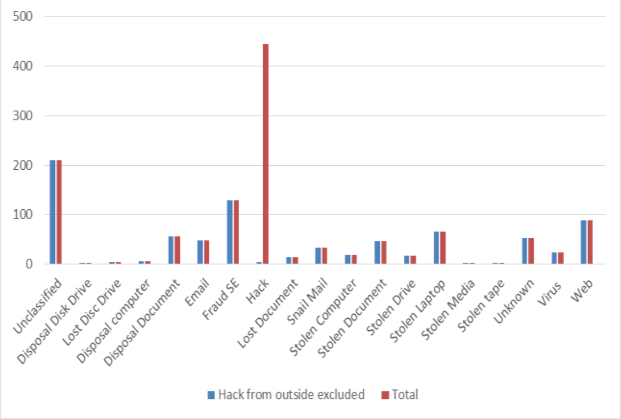

Fig 1. Distribution of data breaches types reported in 2014

A. Multi Tenancy

Multi tenancy is built for reasons like allocation of resources, sharing of memory, storage and distributed computing. It provides effective utilization [9] of hardware components, and maintain cost is very low. It gives distribution of resources, services and application with other components residing on same physical/logical platform at service providers. Thus, it breaches the confidentiality of data and leakage of information and this causes the possibility of attacks.

B. Insider Attacks

Cloud computing is a multitenant based model that is provided by the service provider. So, the threat of leakage of information arises within the organization. There are no rules for hiring cloud employees. So, an organization can easily hack by the third-party vendor, due to this the data of one organization cannot be safe. It’s leads loss of information of user, confidentiality, integrity and security. This attack is difficult to defend and the solution of this attack is no found yet [17].

C. Outsider Attacks

This is also one of the major issues in an organization. Data are resided in server and this confidential data of an organization in open to other. In Clouds there many interfaces, so cloud is differed from a private network. One of the disadvantages is that hackers and attackers to exploiting the API, weakness and this result breaking in connection.

D. Elasticity

When a system is adaptable to changing environment. In these resources are provisioned by the user as their requirement. In this synchronization of available resources and current demand occurs. It implies scalability, and users are able to scale up and down as requirement. Due this scaling tenants use a reusable resource.

E. Security Performance and Optimization

The system adopts Security Measures which may affect the performance of underlying services badly. So, while applying this security measures we should have check the system performance parameter also. So we should try to make a proper balance between both.

F. Information Integrity and Privacy

In a cloud environment, various organizations put their data on server but some flaws in the security of cloud infrastructure occurs. There is breaches of information privacy, integrity and authentication issues come up.

G. Network level attacks

During resource pooling process all data or services flow over the network needs to be secured from attacker to prevent the breaching of sensitive information or other susceptibilities [10].

a) Man in the Middle attack: It is also a category of eavesdropping. The attacker set up the connection between both victims and makes conversation. Attacker making believe that they talk directly but infect the conversation between them is controlled by attack.

b) Brute force attack: In this attack when attacker want to find the password it will try all possible combination of password until correct password not found.

c) Reply attack: In this attack valid data transmission is repeated or delayed due to malicious or fraudulent activity.

d) Distributed denial of service attack: In this attack, servers is down due to huge amount of network traffic. This attack is classified into two broad categories based on protocol level which they targeted one is Network level attack and another is application level attack.

e) Byzantine failure: It is a malicious activity which done at a server or a set of servers to degrade the performance of cloud.

f) Network probe: It is used to find out the possible topology of the network which contain IPs and server. It's used to attack for a sub group in the network.

H. Hardware Based Attack

It is one of the most frequently discovered vulnerabilities in cloud which direct result of language and programmes that are as follows.

a) Trojan horses/Malware: They are the unauthorized program that are contained or injected by malicious user within valid program to perform unknown and unwanted function. Unlike viruses it does not replicate themselves.

b) XML Signature wrapping Attack: Protocol like SOAP that use XML format to transfer the request for services are attack by these types of attacks. In this, attack moves the original body of SOAP message to newly inserted wrapping element writing within SOAP header attack perform in new body.

V. TECHNIQUE TO SECURE DATA IN CLOUD COMPUTING

A. Encryption Algorithm

We that cloud service provider encrypt user's data using a strong encryption technique [11] but in some circumstances encryption accidents can make data completely useless and on the other side encryption it also complicated. As this task is challenging cloud provider must provide proof that encryption technique were design and properly tested by knowledgeable and experience authority.

B. Authentication and Identity

The most common method of authentication of users is cryptography. Through cryptography, authentication is provided between communicating systems [13]. Passwords is one of most common form of authentication of users individually. Other form authentication is security token, or in the form a biometric like fingerprint etc. This traditional identity approach is not sufficient respect to cloud environment. When the enterprise uses multiple cloud service providers (CSPs). In this synchronizing of identity information not scalable. Infrastructure is also one of major concern when we shifting toward traditional approach to cloud-based.

C. Scrutinize Support

Checking of illegitimate activities is a difficult task. When users store their data in the provided cloud, they store data in server and they don't have the information where the data is stored. Therefore, cloud service provider must provide inspection tools to the users to scrutinize and control various policy implementation.

VI. SECURITY COSIDERATIONS

As the IT industry more attractive and useful to the users, if implementation of a cloud computing is not managed properly, can present a number of risks to the enterprise. Many of these risks can have a direct impact on business operations, so it is important to take appropriate mitigating in this process. Figure 1 provides a list of the operational risks related to the implementation of Cloud computing.

. Table 1. A comprehensive study on cloud threats and solutions

Threats	Effects	Affected Cloud Services	Mitigation Strategy
Insecure API and interfaces	Improper authentication and authorization, wrong transmission of content.	SaaS, PaaS and Iaas	Data transmission is in encrypted form, Strong access control and authentication mechanism.
Insider Intruder	Penetrate organizations resources, damage assets, loss of productivity, affect an operation.	SaaS, PaaS and Iaas	Use agreement reporting and breaching notification, security and management process transparency.
Data loss and leakage	Personal sensitive data can be deleted, destructed and corrupted.	SaaS, PaaS and Iaas	Provide data storage and backup mechanism.
Identity theft	Intruder get identity of valid user to access the resources and other benefits of user	SaaS, PaaS and Iaas	Use strong multi-tier passwords and authentication mechanisms
Risk profiling	Internal security operations, security policies, configuration breach, patching, auditing and logging	SaaS, PaaS and Iaas	Acknowledge partial logs, data and infrastructure aspect, to secure data use monitoring and altering system
Shared technology issues	Interfere one user services to other user services by compromising hypervisor	Iaas	Audit configuration and vulnerability, for administrative task use strong authentication and access control mechanisms
Abusive use of cloud computing	Loss of validation, service fraud, stronger attack due to unidentified sign-up	PaaS and IaaS	Observe the network status, provide robust registration and authentication technique

VII. CONCLUSION

Cloud computing is the effective technology which depend on cost, time and performance. It gives benefit to the users of cloud and of course the practice of cloud computing will surely will increase more in next few years. In this paper we have discussed and examine the basic of cloud computing and issues regarding securities in the cloud computing. Some security issues are the very crucial in the cloud computing. Privacy and integrity of data are the especially key concern security issues. In the cloud as data is stored in server and we don't know the exact location of the data resided, due to this data stored in the cloud has a threat of being accessed or theft by unauthorized person during transmission.

REFERENCES

[1] I. Foster, Y Zhao, I. Raicu, and S. Lu, "Cloud Computing and Grid Computing 360-degreecompared[C]", in Grid Computing Environments Workshop, 2008, pp. 1-10.

[2] Rich Wolski, Daniel Nurmi, Chris Grzegorczyk, Graziano Obertelli, Sunil Soman,Lamia Youseff, Dmitrii Zagorodnov, "The Eucalyptus Open-source Cloudcomputing System ", 2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid, CCGRID 2009, pp: 124-131.

[3] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing", Technical Report No. UCB/EECS-2009-28, 2009.

[4] "NIST Cloud Computing Definition", NIST SP 800-145.

[5] Enrique Jimenez Domingo and Minguel Lagares Lemos, CLOUDIO: A Cloud Computing-oriented Multi-Tenant Architecture for Business Information Systems In Proc. of the 23rdInternational Conference on Cloud Computing pages 532-533.IEEE, 2010.

[6] D.G. Cameron, R. Carvajal-Schiaffino, A.P. Millar, C. Nicholson, K. Stockinger, F. Zini, Evaluating scheduling and replica optimisation strategies in OptorSim, in:Proceedings of the Fourth International Workshop on Grid Computing (Grid2003), IEEE CS Press, Los Alamitos,CA, USA, Phoenix, AZ, USA, 2003.

[7] Rajkumar Buyya, Rajiv Ranjan, Rodrigo N. Calheiros, "Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities", in The 2009 International Conference on High Performance Computing and Simulation, HPCS 2009, pp:1-11.

[8] Juefu Liu, Peng Liu, "Status and Key Techniques in Cloud Computing", in Proceedings of 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE) , pp: V4-285– V4-288.

[9] Chang Jie Guo, Wei Sun, Ying Huang, Zhi Hu Wang, Bo Gao , "A Framework for Native Multi-Tenancy Application Development and Management''2007 9th IEEE International Conference on Ecommerce Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services..

[10] C. Hong, M. Zhang, and D. Feng, AB-ACCS: A cryptographic access control scheme for cloud storage, (in Chinese), Journal of Computer Research and Development, vol. 47, no. 1, pp. 259–265, 2010.

[11] William Stallings, Cryptography and Network Security Principles and Practice, fifth Edition, Pearson Publication

[12] Enrique Jimenez Domingo and Minguel Lagares Lemos, CLOUDIO: A Cloud Computing-oriented Multi-Tenant Architecture for Business Information Systems In Proc. of the 23rdInternational Conference on Cloud Computing pages 532-533.IEEE, 2010.

[13] D. Feng, Y. Qin, D.Wang, and X. Chu, Research on trusted computing technology, (in Chinese), Journal of Computer Research and Development, vol. 48, no. 8, pp. 1332–1349, 2011.

[14] H. Zhang, L. Chen, and L. Zhang, Research on trusted network connection, (in Chinese), Chinese Journal of Computers, vol. 33, no. 4, pp. 706–717, 2010.

[15] G. Wang, F. Yue, and Q. Liu, A secure self-destructing scheme for electronic data, Journal of Computer and System Sciences, vol. 79, no. 2, pp. 279–290, 2013.

[16] S. Qamar, N. Lal and M. Singh. Deelman, G Singh (2010). Internet Ware Cloud Computing: Challenges. (IJCSIS) International Journal of Computer Science and security, Vol. 7, No. 3, March 2010.

[17] Naresh vurukonda and B.Thirumala Rao, in 2nd International Conference on Intelligent Computing, Communication & Convergence, ICCC 2016,