A Review of Cloud Computing: Selected Security Issues and Techniques

Tahir Hakim

Depatment of Manangement Information Systems
College of Business Administration, Jazan University, Kingdom of Saudi Arabia.

Abstract : With the emergence of cloud computing being the new trend in information technologies, it has posed a serious threat to the security, resulting in the deterioration of the effectiveness of traditional protection mechanisms. No standard security model or framework can be found in cloud computing when it deals with the transmission of sensitive data and critical applications. Due to the security reasons in cloud computing environment, the users have lost their trust in cloud. There are various security issues in cloud computing like multi- tenancy, elasticity, Security Performance and Optimization, etc. Some of the issues will be reviewed in this paper. This paper will also discuss the existing security techniques in order to secure cloud and make the researchers and professionals aware about various security threats.

IndexTerms **-Cloud Computing, Security Issues, Security Techniques**.

I. INTRODUCTION

Cloud Computing can be defined as a mix approach of grid and utility computing which when put together form a collection of dynamically inter connected computers. Many changes are undergone by computing from grid computing to cloud computing and a new computing model is thus proposed by the researchers, which is called as Cloud Computing, commercializing its previous models. Cloud computing environment, being the major achievement of computing, can bring changes in IT industry, which could make the IT industry more resourceful and attractive to the users. It could also bring changes in the livelihood of people and their work style.

Cloud computing being a new and evolving field, it caters to the industries with new technology. There are two types of applications in cloud computing, which are, PAAS (platform as a service) and IAAS (infrastructure as a service). PAAS provides the configuration and reconfiguration of the servers, which are the physical/virtual machines. According to cloud computing, applications are accessed by internet, for which, powerful servers and large data centers are needed and the main differences between cloud computing and traditional computing is elasticity and scalability. This paper focuses on several security threats associated with cloud computing long with their counter measures.

II. CLOUD SERVICE MODELS

a. **Software as a Service**

Software as a service is sometimes also known as “on demand”. It is a software delivered model in which without any interaction with the cloud service provider, the user individually furnishes its resources depending on the requirement. SAAS is accessed by a customer via web browser and it is often updated in comparison with traditional software. It is now a delivery model for various applications, such as, Payroll Processing, CRM (Customer Relationship Management), HRM (Human Resource Management and Service), etc.

b**. Platform as a Service**

It provides a platform for computing as well as a solution stack as service. In this service model, the soft wares are created by the customers using tools and libraries that the service provides through a provider. It also provides the customer with the virtualized servers in order to run existing applications. The server is also provided with the hardware storage and networking by the provider. The main advantage of this service is that many developers can work simultaneously on one project.

c. **Infrastructure as a Service**

Virtual computing resources are provided by this service over internet. Furthermore, the consumer can furnish the processing, storage, hardware, servers, and network , etc. where the soft wares like operating systems and applications can be run.

III. CLOUD DEPLOYMENT MODEL

a**. Public Cloud**

Public cloud is one of the computing models based on the standard computing model in which the general public is provided with the utility computing over internet on payment basis and the major benefits of this model are scalability and inexpensive resources being properly utilized**.**

b. Private Model

This type of model is restricted to a single organization only for privacy reasons. It also has the benefits of scalability and self-service.

c. **Community Cloud**

This type of model is a multi-tenant infrastructure whose infrastructure is shared by the multiple organizations and a specific community is supported having common computing concerns.

d. Community Cloud

In this type of computing model, the infrastructure is shared by at least one public and one private cloud.

IV. CLOUD SECURITY ISSUES

The four models discussed above have certain security issues and concerns. In most of the applications, the data gets stored in the servers, which is sometimes confidential and securing data is of vital importance. Thus, there are many challenges regarding the security of the confidential data stored and the leakage of such data can be fatal to many computing systems, like the year 2014 marks the highest year in data breaches with about 740 million records being leaked, which is the highest till now in computing history, which is also called as the year of mega breaches and identity thefts.

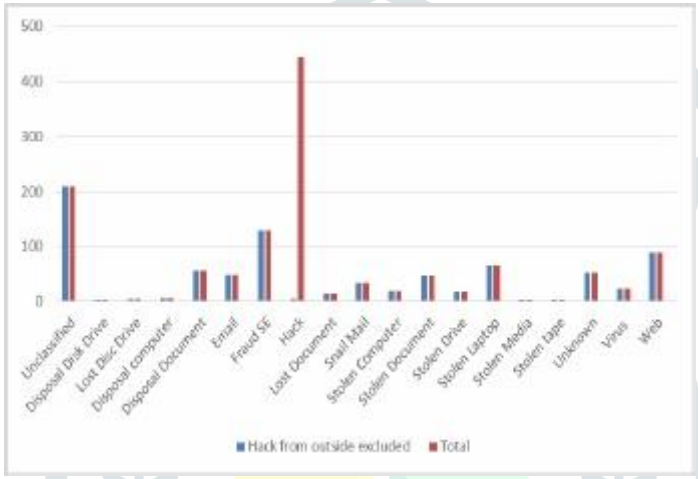

Fig 1 Distribution of Data Breaches reported in 2014

a. Multi Tenacity

Multi tenacity is built or created for the allotment of resources, memory sharing, storage as well as for the storage and distributed computing. The maintain cost of Multi- Tenacity is very low in addition to being the effective in utilizing the hardware components. It provides the distribution of resources, services and applications with other components residing on same physical or logical platform at service providers. Thus, the confidential data is breached and the information is leaked which results in the possibility of serious attacks.

b. Insider Attacks

Cloud computing being a multitenant based model, provided by the service provider, the threat of breaching or leakage of the information is within the organization. There are no rules while hiring the employees for cloud, which results in the organization being easily hacked by a third party vendor, which makes the data very unsafe of an organization. Thus, it leads to the loss of user's information as well as his confidentiality, security and integrity. This kind of attack is difficult to defend and there has not been any solution found yet to such attacks.

c. Outsider Attacks

It is one of the major issues in any organization. Data is stored in the server and this data is open to other organization to be accessed. There are many interfaces in clouds, which makes it different from the private networks. The hackers can exploit the API, which in turn results in the breakage in the connections.

d. Elasticity

The users use the system as per their requirements, when the system is adaptable to changing environment, which implies the scalability and the users are able to scale up and down as per their requirements because of which the reusable resources are used by the scaling tenants.

e. Security Performance and Privacy

The performance of the underlying services is affected badly when the system adopts the security measures. Thus in the process of applying the security measures, the system performance parameters should be checked. Thus a proper balance should be made between both.

f. Information Integrity and Privacy

When the data is put on the server by various organizations, in a cloud environment, some flaws occur in the security of cloud infrastructure. There are breaches in the information privacy, security and integrity as well and the problem of authentication arises.

g. Network level attacks

All the data or service flow over the network needs to be secured from the attacker during resource pooling process in order to prevent it from breaching of sensitive information, etc.

V. TECHNIQUES TO SECURE DATA IN CLOUD COMPUTING

a. Encryption Algorithm

The user's data in encrypted by the cloud service provider by using the strong encryption technique but due to some unavoidable circumstances, encryption accidents happen, which make the data useless completely. Thus the cloud provider should be asked to provide a proof showing that the encryption technique design is properly tried and tested by an experienced authority.

b. Authentication and Identity

Cryptography is the most common method of authentication for the users. Authentication is provided through cryptography between the communicating systems. Passwords is one of the most common and important form of authentication for users individually. Security token or biometric like fingerprint, etc. is the other form of authentication and in cloud computing environment, the traditional identity approaches is insufficient when multiple cloud service providers used by the enterprise. While moving from traditional approach to cloud-based approach, infrastructure becomes one of the major concerns.

c. Scrutinize Support

It is a difficult task to keep a check on the illegitimate activities. The users have no idea of where the data is stored when they store their data in the provided cloud in the server. Thus, the cloud service provider must provide the inspection tools to the users to scrutinize and control various policy implementations.

VI. RISKS AND SECURITY CONSIDERATION

As the IT industry being more attractive and useful, if the implementation of a cloud computing is not managed properly, it can present a number of risks to the enterprise and most of these risks can have a direct impact on the business operations. Thus, it becomes necessary to take appropriate measures in this process. Table 1 provides a list of operational risks related to the implementation of cloud computing.

Table1. A comprehensive study on cloud threats and its 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 transmission
Insider Intruder	Penetrates organizations' resources, damages assets, loss of productivity, affects 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 gets 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	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

Depending on the cost, time and performance, cloud computing is an effective technology. The users of cloud are benefitted by its usage and the practice of cloud computing is surely to increase in more in next coming years. This paper focused on the basic cloud computing and issues related to securities in cloud computing and some of them are very critical. Privacy and integrity of data are the key concern security issues. As the data is stored by the user in the cloud, the user does not know where it is stored in the server nor does the user know the exact location of the data resided because of which there is a threat to the stored data being accessed or stolen by an unauthorized person during the 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 Cloud computing System",*20099th IEEE/ACM International Symposium on Cluster Computing and theGrid* , 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 23rdInternationalConference 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 optimisationstrategies in OptorSim, in: *Proceedings of the Fourth International Workshop on Grid Computing (Grid2003)*, IEEE CS Press, LosAlamitos,CA, USA, Phoenix, AZ, USA, 2003.

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

.

[8] 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.

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

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

[11] 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.

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

[13] 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.