Sindh Univ. Res. Jour. (Sci. Ser.) Vol.49 (004) 831-834 (2017)

http://doi.org/10.26692/sujo/2017.12.00167

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

Cloud Computing Security

S. SHORO, S. RAJPER, B. BALOCH*

Department of Computer Science, Shah Abdul Latif University, Khairpur, Sindh, Pakistan

Received 4th November 2016 and Revised 19th August 2017

Abstract: Cloud computing is a computing framework and software model for empowering ubiquitous access to shared pools of configurable assets i.e. Server, networks, services and storage applications which can be quickly provisioned least managements activities often over the web. Cloud computing is a moderately new innovation that will only become widespread and very much researched. Cloud computing do not requireextra ordinary equipment for customers and offers ease of use. It is beneficial for clients. It is accepted that Cloud Computing has many potential advantages but at the same time there are some security issues need to resolve. The undertaken study aims to present the various Cloud Service Delivery Models, Cloud Deployed Models and mainly focuses on Security issues at each service model. This study will be helpful for the scholars, researchers and academicians.

Keywords: Cloud computing, Infrastructure, Cloud Service delivery models, Cloud deployment models, Cloud Computing Security, Data Security.

1. INTRODUCTION

Cloud Computing is the new pattern of computing that comprises conveying hosted services over the internet. Cloud Computing has increased widespread popularity in industry, Business and academia. (Sadiku, *et al.,* 2014) CloudComputing is an innovation having information and its application by utilizing internet and centralized remote servers. (Priyanka *et al.,* 2012). It was first presented in 2006 as "Elastic Compute Cloud" by Amazon. The idea of Cloud Computing structureis derived from the cloud-shaped symbol. (Sukhpal *et al.,* 2013) Cloud Computing offers the tools and technologies to manufacture intensive parallel applications with some reasonable prices as compared to traditional parallel computing techniques. (Mohammad., 2012). The cloud computing exhibits the essential characteristics i.e.on-demand self-service, broad network access, Resource pooling, rapid elasticity, measured service. (Neha *et al.,* 2014) There are several approvals to implement cloud computing but still it consist of some holes that make implementation difficult. By using the Cloud Computing the organizations reduces their IT cost and employees can easily access the data. The cloud computing permits clients and organizations with numerous computing proficiencies to store and display data and that data is stored on servers maintained and controlled by a cloud service provider i.e. I cloud. (Haghighat, *et al.,* 2015) Cloud service provider offers area to utilize and generate their web services just like internet server providers offers the high speed access to the internet. Many cloud service providers can share their data with third parties due to involvement of third party the security issues occur. Cloud Security refers to the set of rules, technologies, and control organized to protect data, applications, and the connected framework of cloud computing. The data security is a major risk of Cloud Computing which needs to be resolved. Cloud computing service providers must ensure their clients for data security and relief from numerous attacks.The goal of this study is to present various Cloud services models, Cloud deployment models and mainly focuses on Securityissues on Service Delivery Models of cloud computing. This will be beneficial for the researchers, scholars and academicians.

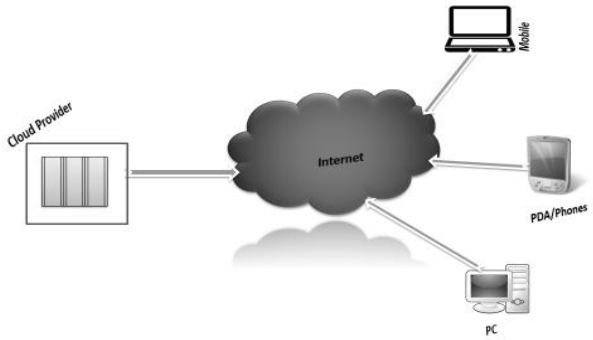

Fig.1 Cloud Computing Infrastructure

2. RELATED PAST WORK

Lot of research has been done regarding the Cloud Computing but (Ogigau-Neamtiu, 2012), (Ali, *et al.,* 2015), (Sean *et al.,* 2012), (Meiko *et al.,* 2009), (Subashini, and Kavitha, 2011) have mentioned the

++Corresponding author's email: shorosaima@gmail.com, samina.rajper@gmail.com
*University of Tando jam, Sindh, Pakistan

different models and security issues of Cloud Computing, while (Ankur *et al.,* 2013), (Rai *et al.*, 2014), (Suresh *et al.*, 2012) introduces different technologies and algorithms to resolve the security issues. The currentreview by IEEE and Cloud Security Alliance describes the rapid adoption and impact of cloud computing (Zia, *et al.*, 2012).

3. CLOUD SERVICE DELIEVRY MODELS

The classifications of Cloud Service Delivery Models are mentioned as "SPI Model" stands for the Software, Platform and Infrastructure respectively.

A- Software as a Service (SaaS): This model delivers access of complete application running on cloud by using the web portal or software oriented architecture i.e. Domain Consistence Server (DCS) or Main Consistence Server (MCS). (Vijayapriya, 2013). The clients doesn't manage or temper the basic framework of cloud containingoperating systems, server, network, storage.ie Caspio, Google Apps, Sales force, Nivio, Learn.com.

B- Platform as a Service (PaaS): This model summarize the atmosphere for the development and provisioning of cloud applications by using programming languages and tools supported by cloud service provider. Client doesn't control or manage the basic framework of cloud but has control over the applications development environment configurations i.e. Google App Engine, Force.com and Microsoft Azure.

*C- Infrastructure as a service (IaaS):*This model allows the client to use important IT resources.The client doesn't manage or control the basic cloud framework but has control over operating systems, storage, and arranged applications; and limited control of networking components (host firewalls). It is a platform which gives availability of devices to the businesses at pay-per-use service.ie Amazon Elastic Cloud, Amazon S3, Go Grid,Computing (EC2). Illustrated in **(Fig. 2).**

Fig. 2. Cloud Service Delivery and Deployment Models

4. CLOUD DEPLOYMENT MODELS

Cloud Computing Models are classified into three main Cloud Deployment Models depends on as per demand:

A-Private Cloud: Private cloud is a wordwhich is used todefine cloud computing on private networks. The cloud is operated by single organization andits designated participants. It is different from the public cloud because its assets and applications are accomplished by the association itself. This cloud is much more secure than the public cloud.I.e. Amazon Elastic Cloud, Amazon S3, Go Grid and Computing (EC2). (Vijayapriya, 2013).

B- Public Cloud: This cloud framework is constructedfor public or large group of industries and is owned by services sellers. Public cloud illustrates the cloud computing in the traditional typical logic, whereby assets are managed on self-service basis. It is typically based on a pay-per-use model. ("Enterprise Cloud Computing: Transforming IT." Platform Computing, 2010) Public cloud is less secure than other models. The services of this cloud may be free. i.e. Eucalyptus Systems.

C- Hybrid Cloud: The framework of hybrid cloud us composed of two or more clouds (Public or Private).Hybrid cloud is a private cloud are managed as a single unit, and bounded by a secure network. ("Demystifying the cloud. Important opportunities, crucial choices.", 2009) Gatner, Inc introduces a Hybrid Cloud Service as a Cloud Computing Service i.e. (AWS) Amazon Web Services. These models are also illustrated in **(Fig.2).**

5.CLOUD SECURITYAND ITS ISSUES AT EACH SERVICE MODEL

Cloud Security belongs to the set of rules, technologies, and control sorted out to protect data, applications and the connected framework of cloud computing. Cloud Computing security issues are classified into two groups: security issues encountered by cloud serviceproviders andissues encountered by their customers.There are different security issues at each service model are discussed below:

A- Security issues in SaaS: In SaaS the client totally depends upon the service provider for security dealings and it is difficult to assure that the application will provided on the time when it is needed. In SaaS the organizations data is present on data center of service providers where the data of other organizations is also presented if the service providerprovides the services through public cloud the provider might replicate the data at various places to maintain high level of availability. The other issues faced on this model are listed below:

- Network security
- Data security
- Data locality
- Data Segregation
- Data authentication and authorization
- Data integrity
- Data access
- Data breaches
- Data Confidentiality

- Data availability
- Backup
- Virtualization and vulnerability
- Web application security
- Identification and sign- out process

B- Security issues in PaaS: At this model the service provider allow the clients to build their applications but the security below the application layer like host and network intrusion prevention will still under the control of service provider but they have to offer solid assurance that the data is inaccessible between applications. The application's security is only controlled by the service providers. If the hackers can hack the infrastructure of an application then it is very easy for them to hack its visible code. (Neha and Prachi, 2015).

C- Security issues in IaaS: in this model service provider hastemper on security. According to theory virtual machines are used to resolve security concerns but still there are several security issues. (CR., 1973) (Gajek, *et al.,* 2007) Security responsibilities of service provider and consumers are different from each other. Amazon Compute Cloud (EC2) infrastructure describe the providers issues i.e. Environmental security, Physical security, Virtualization security and the consumers issues are related to IT systems i.e. Data security, Applications security, operating system security.These issues are also described in **(Table-1).**

Table-1Security Issues in different Service Models

Service Models	**Security Issues**	**Examples**
Software as a Service (SaaS)	Data security,Data Segregation,Data locality,Data access, Data authentication authorization, Data integrity,Data confidentiality,Data breaches,Data availability,Backup, Virtualization, vulnerability Identification and sign- out process,Web application security, Network Security.	Caspio, Google Apps, Google Docs, Gmail, Salesforce, Nivio, Learn.com, Yahoo etc.
Platform as a Service (PaaS)	Virtual machine off generates security issues. If the hackers can hack the infrastructure of an application then it is very easy for them to hack its visible code	Google App Engine, Microsoft Azure, SQL Azure, Force. Cometc.
Infrastructure as a Service (IaaS)	Environmental security, Physical security, Virtualization security are provider's issues. Data security, Applications security, operating system security are consumer's issues.	Amazon Elastic Cloud, Amazon S3, Windows Azure, Go GridComputing (EC2), Amazon web services etc.

5. DISCUSSION

From this study it is found that Cloud Computing is being increasingly used in this technological era. It is gaining popularity in Industry, Business and Academia. It is moderately a new innovation which is very much researched now a days. Cloud Computing places the data and applications on centralized remote server which can be accessed by using the internet. From the survey conducted by IDC in 2008 it is found that more than seven IT systems are migrated to the cloud. In 2013 it was reported that the Cloud Computing adaption growth rates are increasing 50% per year. And recent research tells that many organizations achieved 18% IT budget reduction and 16% data center power cost reduction from Cloud Computing. Whereas some researchers addressed that Cloud Computing is not a secure service because when we share our data to third party on wide area over thousand number of devices by different unrelated users its security issues increases i.e. Data integrity, Data confidentiality, network security visualization and vulnerability, Data access and Data breaches etc. are also mentioned above. Despite of this the private cloud installation motivates the users to adopt cloud computingbecause the users have control on the framework and eludeto lose the security temper.

6. CONCLUSION

The goal of this study is to illustrate the various models and security issues and challenges faced on these service models. From this study it is found that Cloud Computing is beneficial for Client, Costumers and Business. Different issues from network layer to the application layer are found and need attention oncloud data security. Thedata integrity and confidentiality should maintain to secure itCloud Computing there are two aspects of security one is maintaining high security of Cloud data and other is security attacks prevention risen by Cloud itself. Now a days Cloud Computing adoption is increasing rapidly and the service providers are working on resolving the issues faced by the clients with different techniques so the security control techniques might be the best area for the future work.

REFERENCES:

Ali M., S. U. Khan, and V. Vasilakos, (2015) "Security in Cloud Computing: Opportunities and Challenges," Information Sciences, vol. 305, 357-383.

Ankur M., R. Mathur, S. Jain, and J. S. Rathore, (2012) "Cloud Computing Security," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 1, no. 1, 36-39, 2013.

Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi (INDIA).

Demystifying the cloud. Important opportunities, crucial choices.", (2009) " Global Netoptex Incorporated, 4-14.

Gajek S., I. Liao J. Schwenk, (2007) "Breaking and fixing the inline approach," proceedings of the ACM workshop on secure web services. Newyork, 37-43.

Haghighat, M. S., S. Zonouz and M. Abdel-Mottaleb (2015) "CoudID: Trustworthy Cloud-Based and Closed Enterpise Biometric Identification," Expert Systems with applications, vol. 42(21), 7905-7916.

Hamadaqa, M. (2012) "Cloud Computing Uncovered: A Research Landscape Elsevier Press, 41-85.

Jensen, M., J¨org Schwenk, N. Gruschka, and L. L Lacono, (2009) "On Technical Security Issues in Cloud Computing," IEEE International Conference on Cloud Computing, 109-116.

Metha, C R., (1973). "Virtual machines and data security," in:Proceedings of the workshop on virtual computer systems Newyork, 206-209.

Neha M., and J. P. Tripathi, (2014) BIJIT - BVICAM's International Jour. of Information Technology.

Neha K., N. I. Prachi, (2015) "Security Threats In Cloud Computing," Interntional Conference on Computing , Communication and Automtion (ICCCA), 691-694.

Ogigau-Neamtiu, F. (2012) "Cloud Computing Security Issues," Journal of Defense Resource Management, vol. 3, no. 2(5), 141-148.

Priyanka A., A. Singh, and H. Tyagi (2012) "Analysis of performance by using security algorithm on cloud network," International Conference on Emerging trends in Engeneering and Management (ICETM), 23-24.

Rai, P. K., R. K. Bunkar, and V. Mishra, (2012) "Data Security and Privacy Protection Issues in Cloud Computing," IOSR Journal of Computer Engineering (IOSR-JCE), vol. 16, no. 1, 39-44, 2014.

Singh, S., and I. Channa (2013) International Journal of Cloud Computing and Services Science (IJ-Closer), vol. 2, no. 1, 73-84.

Sadiku, M., S. Musa, and O. Momoh, (2014) "Cloud Computing Opportunities and Challenges," IEEE Potentials, vol. 33(1), 34-36.

Sean C., and K. Curran, (2012) "Cloud Computing Security," International Journal of Ambient Computing and Intelligence, vol. 3(1), 14-19.

Subashini, S. and V. Kavitha, (2011) "A survey on security issues in Service delievery models of Cloud computing," Journal Of Network and Computer Applications, vol. 34, 1-11.

Suresh K. S., M. Tech, and K. V. Prasad (2012) "Security Issues and Security Algorithms in Cloud Computing," International Journal of Advanced Research in Computer Science and Software Engineering , vol. 2, no. 10, 110-114.

Vijayapriya, M. (2012) "Security Algorithm In Cloud Computing: Overview"," International Journal of Computer Science and Engineering Technology (IJCSET), 2013.

Zia, A., A. khan and M. Naeem, (2012) "Identifying key Challenges in Performance Issues in Cloud Computing," Journal of Modern Education And Computer Science , vol. 4, no. 10-12.