Literature Review: Cloud Computing–Security Issues, Technologies and Challenges

D.Jothipriya[#1], Dr. A.Akila[*2]

[1]*M.Phil. Scholar, Dept of Computer Science, Vels University, Chennai*

jothi.gopal@gmail.com

[2]*Assistant Professor, Dept of Computer Science, Vels University, Chennai*

Abstract— Cloud computing is drastically increasing so to make cloud computing more popular the very first step for the organization is to identify exact place where the cloud related threats lie. The changes from server to service based technology brought a increasing change in computing technology. The developments have created new security vulnerabilities, including security problems whose full impressions are still rising. This paper presents an overview and study of cloud computing, with several security threats, security problem, currently used cloud technologies.[1],[4]

Keywords— Cloud Computing; Threats; Security problems; Service Models.

1. Introduction

Cloud computing is collection of resources that are being given on demand. Cloud computing gives new ways to provide services. Business is operated using these new, technical opportunities. Cloud computing is a collection of resources and services provided by provider through internet. As the cloud computing is rapidly growing this also leads to major security problems. Lack of security is the only threat in wide adoption of cloud computing. The drastic growth of cloud computing has brought many security challenges for users and providers.[5],[7]

2. Cloud Service Models

2.1 Cloud Software-as-a-Service

It is a software distribution scheme which gives access the software and its functions distantly as a web-based service. SaaS provides organizations to get into business functionality a low cost normally less than paying for licensed applications in view of the fact that SaaS charges are built on a monthly fee. As the software is hosted remotely users need not pay for additional hardware. SaaS removes all opportunities for organisation to handle the installation, set-up, daily storage and maintenance.[8]

2.2 Cloud Platform-as-a-Service

The capability given to the users to deploy onto the cloud infrastructure. PaaS model, cloud provider brings a computing platform, naturally consisting of OS, Programming Language execution environment, database and web servers. The developers can develop and run their program results on cloud platform with no cost and difficulty.[9]. Users uses these platforms which is being Integrated Development Environment (IDE), so as it consists the editor, compiler, build and deploy features to develop their applications.
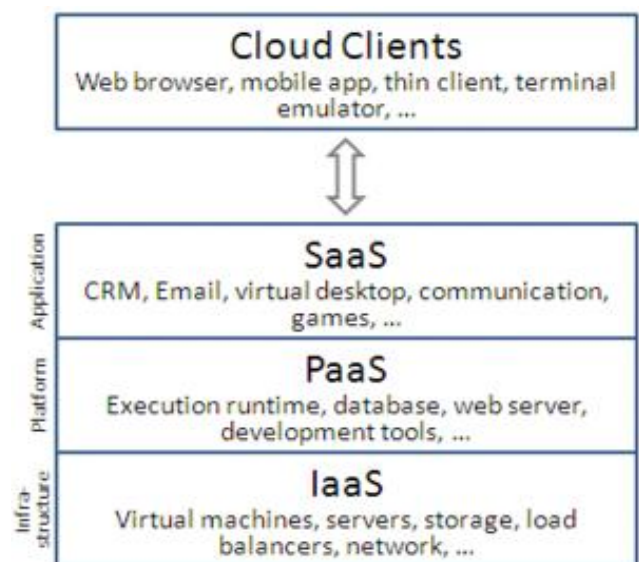

Fig.1: Cloud Service Model

2.3 Cloud Infrastructure-as-a-Service

The IaaS provider gives the access of the services of servers, storage, OS and other networking. The end user takes on these provided services based on their needs and pay for what they have used. The user is able to deploy and run any software, which comprise Operating Systems, applications [2] Flexibility and scaling are the rights of the end user, not the supplier. Amazon Elastic Compute Cloud is an IaaS model that facilitates growing compute volume, on demand, in the cloud. It allows users to influence Amazon's infrastructure with no pay in advance investments. Amazon EC2 decreases the clock needed to control of and boot latest server copies and allow users to immediately increase space – equally up and down as their computing needs differ.
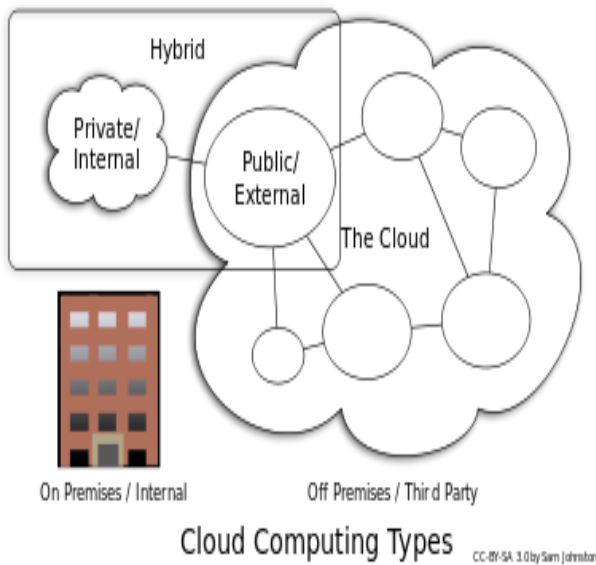
3. Cloud Deployment Models

Fig.2 :Cloud Computing Types

3.1 Public Cloud

A cloud is to be titled as public cloud when the services (like applications, storage) are being given through internet that are available to anyone who can access it publically. The identified benefits of the Public cloud may considered as pay based   usage mode or any other purchasing schemes .[6]

3.2 Private Cloud

 The private cloud is consider as an infrastructure which provides the services to one organization, whether it is managed internally or by a third party.

3.4 Community Cloud

It comprises sharing of infrastructure between organizations of same group of people.

3.5 Hybrid Cloud

 The hybrid cloud is a collection of both private and public cloud options.That remains unique entities but is collectively by the uniform or proprietary application.

4. Cloud Security Issues

 While cost and ease of use are the two main advantages of the cloud computing, there are some major problems that need to be noticed when allowing crucial application and secret data to public and shared in cloud environment[14].

We should say that Security and privacy are the key challenging problems in the cloud computing. Here are some security problems, we have presented in this paper.
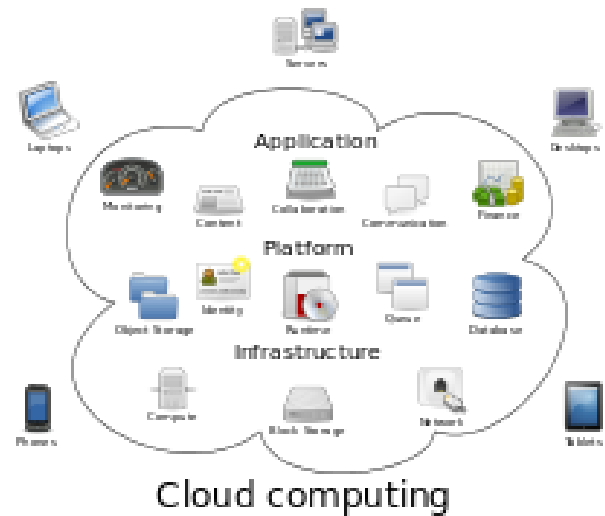

Fig.3: Cloud Security issues

4.1 Data Confidentiality Problem

 Confidentiality is a group of rules that bounds access limits to certain kinds of information. It means that users data are to be kept secret from both cloud provider and other users who is using the service. We must make sure that user's private or secret information should not be used by anyone in the cloud computing, including application, OS, CPU and physical memory. It is clear that user's confidential data is provide to service provider on the following situation only[12].

A. Circumstance 1

 The first situation where user's Information may be produced when service provider knows where their private information is located in the cloud systems.

B. Circumstance 2

 The second situation where user's message may be produced when service provider has the right to access and collect user's private information in the cloud systems.

C. Circumstance 3

 The third situation where user's message may be produced when service provider can find out the meaning of user's information[11] .These are the following circumstances for the service provider to access the user's information and   must know the place of the data in the cloud computing [5]. The service provider know where the user's data is stored and they can access the data.

4.2 Data Availability Issue

When storing data at distant location which is owned by others, data owner may find the issue of system failure of the service provider. And if cloud stops working, data will not be available because it is handled by one service provider. Threats to data availability are overflow attacks causes refusal of service and Direct /Indirect (DOS) attack. The Service Level Agreement(SLA) will not be met when some services are not available[13].

4.3 Data Integrity Issue

It is the "completeness" of the data which is the basic and central needs of technology . Integrity of data and storing of data are very critical and important for the cloud. It proofs the validness and consistency of the data. Therefore cloud storage is becoming famous for the outsourcing of daily management of data[4]. The cloud provider should give assurance to the user that if their data is stored in the cloud surely .

4.4 Data Security Problem

When we talk about data storage in the cloud computing , the sensitive data of every organisation continues to be there within the organisation boundary . It can be solved by using some encryption techniques for the protection of the data . The data protection needs to be implemented in order to secure data from the following uncertainties[3].

4.5 Trust Issue

Trust is also one of a major problem in cloud computing. Trust comes around assurance and confidence that people, data, objects, information will perform in projected way.When any user stores their data on cloud storage, they must believe the cloud provider so that they don't be afraid to put their data on cloud, like we are trusting and using Gmail server, yahoo server. Therefore cloud provider must provide some techniques to solve with the trust problem and build trust with the users so that many people will be using cloud computing without having any doubt[2].

5. Conclusion

In this paper we have analysed fundamental concepts of cloud computing and security issues in the cloud computing. The privacy and integrity of data are the major security issues. In the cloud the users informations are publically stored but they don't know where it is stored and also the exact location of the data.The data stored has a risk of being utilized by malicious person during storage as well as transmission

References

[1] Mell, Peter, and Timothy Grance. "The NIST definition of cloud computing (draft)." NIST special publication 800.145 (2011): 7.

[2] Pearson, Siani, Yun Shen, and Miranda Mowbray. "A privacy manager for cloud computing." Cloud Computing. Springer Berlin Heidelberg, 2009. 90-106.

[3] Zhang, Qi, Lu Cheng, and Raouf Boutaba. "Cloud computing: state-of-the-art and research challenges." Journal of internet services and applications 1.1 (2010): 7-18.

[4] Voorsluys, William, James Broberg, and Rajkumar Buyya. "Introduction to cloud computing." Cloud Computing (2011): 1-41.

[5] Wang, Lizhe, et al. "Cloud computing: a perspective study." New Generation Computing 28.2 (2010): 137-146.

[6] Iosup, Alexandru, et al. "Performance analysis of cloud computing services for many-tasks scientific computing." Parallel and Distributed Systems, IEEE Transactions on 22.6 (2011): 931-945.

[7] Fernandes, Diogo AB, et al. "Security issues in cloud environments: a survey."International Journal of Information Security (2013):1-58.

[8] Chandrahasan, R. Kalaichelvi, S. Shanmuga Priya, and L. Arockiam. "Research Challenges and Security Issues in Cloud Computing." International Journal of Computational Intelligence and Information Security 3 (2012).

[9] Sen, Santanu Kumar, and Sharmistha Dey. "An Investigation towards Security Threats for Cloud Computing.

[10] Martin, S. Schrittwieser, et al. Dark clouds on the horizon. using cloud storage as attack vector and online slack space¡. Proceedings of the 20th USENIX conference on Security. San Francisco, CA, USENIX Association.

[11] Gruman, Galen (2008-04-07). "What cloud computing really means". InfoWorld. Retrieved 2009-06-02.

[12] Mao, Ming; M. Humphrey (2012). "A Performance Study on the VM Startup Time in the Cloud". Proceedings of 2012 IEEE 5th International Conference on Cloud Computing (Cloud2012): 423. doi:10.1109/CLOUD.2012.103. ISBN 978-1-4673-2892-0.

[13] Dario Bruneo, Salvatore Distefano, Francesco Longo, Antonio Puliafito, Marco Scarpa: Workload-Based Software Rejuvenation in Cloud Systems. IEEE Trans. Computers 62(6): 1072–1085 (2013)[1]

[14] "Defining and Measuring Cloud Elasticity". KIT Software Quality Departement. Retrieved 13 August 2011.