ISSN No. 0976-5697

Volume 7, No. 6 (Special Issue), November 2016

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Survey on issues of Security in Cloud Computing

Geetu
Assistant Professor
Guru Nanak College
Budhlada
single.geetu@gmail.com

Sandhya Vats
Assistant Professor
Guru Nanak College Budhlada
profsandhyavats@gmail.com

Abstract- Cloud computing is one of the most new technology in market. it is a combination of the concept of "software-as-a-service" and "utility computing".it provide convenient and on-demand services to requested end users. Cloud service provider and the cloud service consumer should make sure that the cloud is safe enough from all the external threats so that the customer does not face any problem such as loss of data or data theft. In which user can access their files or data from anyplace using Ainternet. It has several positive impacts like increase throughput, reduce costs, improve accessibility and requires less training but on the other hand it had certain important and critical aspect, and has numerous issues and problem related to the security . In this paper discusses the cloud service consumer such as data, privacy, and infected application and security issues.

I. INTRODUCTION

The Concept of cloud computing took popularity in 1990's though its concepts lasts back to 1960's[1]. Cloud computing technology is a new concept, which provides great opportunities in many areas.it provides services in the form of on-demand services, it's accessible for everyone, everywhere and every time , including clouds referring to the internet and the web. Cloud computing is a concept still young but not so new that. Cloud computing is a collection of computers and servers that are publically accessible via internet [2]. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. Cloud computing provides the variety of internet based on demand services like software, hardware, server, infrastructure and data storage [3]. we focus on some papers that show different risks in the cloud and the different existing solutions that
address these various problems[4].In this paper, we will define cloud computing and its various models. Services, advantages and disadvantages of this technology. This new technology suffers like all computer systems a serious problem that reduces trust between the client and the provider is the security.Sen the last five exposes some challenges facing the cloud.

II. CHARACTERISTICS OF CLOUD COMPUTING

National Institute of Standard and Technology (NIST) describes cloud computing with five essential characteristics such as

On-demand self-service – Cloud provides all needed computing resources as per requirement to user.

Broad network access – User can access cloud services using desktop, laptop, mobile phone etc. over the internet.

Resource pooling – Cloud provider schedules resources to the user as per their requirement.

Rapid elasticity – Cloud computing has ability to quickly allocate and de-allocate the services as per requirement.

Measured service – Cloud providers controlling on usage of resources.

III. SERVICE MODELS

A. Software as a Service (SaaS)

It has the ability to provide user any software running on a cloud substructure. Software is deployed over the internet. In this model customers licenses the applications and the cloud service providers provide the required facility to the end users when they require[3]. Examples may include web browsers and google docs[4].

B. Platform as a Service (PaaS)

Platform can also be provided as a service. In this any kind of platform (i.e. tools, library, services) is provided as a service of which user has no control but he/she can use it[5]. User can easily generate applications by using PaaS provided by CSP[6]. Mostly virtual machines are used in this case. Most preferably various kinds of tools and applications are deployed to facilitate the users [4].

C. Infrastructure as a Service (IaaS)

Infrastructure facilitates the user by providing computing resources where user can run the software without having control on underlying infrastructure but has control over the operating system being used[1]. IaaS may include IT resources such as severs, networking and storage. Users get access to the infrastructure with the help of virtual machines. It provides an elastic architecture which offers high rate of availability[7].

978-93-85670-72-5 © 2016 (RTCSIT)

CONFERENCE PAPER
International Conference on
Recent Trends in Computer Science & Information Technology (RTCSIT-2016)
21st August 2016
Guru Nanak College Budhlada, Punjab India

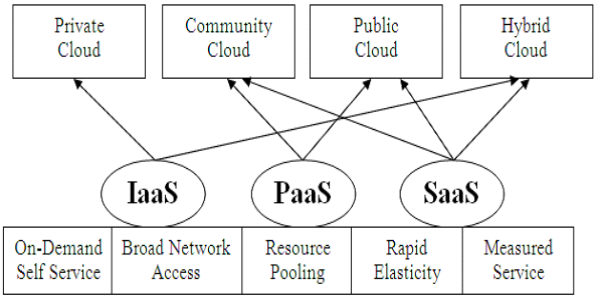

Fig. 1.1 Cloud Structure

IV. DEPLOYMENT MODELS

There are three Deployment Models and are described below:
· Public Model
· Private Model
· Hybrid Model

Public Model: This infrastructure is available to the general public. As the name suggests, public cloud is a model in which resources are generally available to everyone or anywhere.

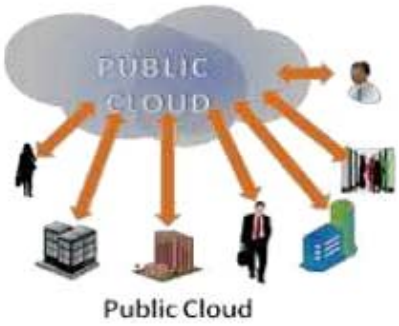

Fig-1.2 Public Cloud

Private Model: This model is developed for the private organizations like one house and an organization and they can use it for their own purpose. This kind of a service is not accessed by everyone.

Fig-1.3 Private Cloud

Hybrid Model: Hybrid Clouds are combination of public and private cloud in a same network. This can be done if private cloud need some important services from the public cloud like Private cloud can store some information on their private cloud and we can use that information on public cloud. In cloud computing, there are many issues but security is the major issue which we will discuss further.

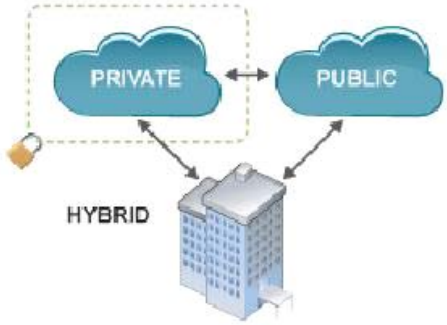

FIG-1.4 Hybridcloud

V. BENEFITS OF CLOUD COMPUTING

1) Increase Throughput – Cloud computing get more work done in less time with less people.
2) Reduce Costs – In cloud computing, user shares computer hardware, software and data so there's no need to spend money on hardware or software.
3) Improve Accessibility – In cloud computing user can access data, files anytime from anywhere via internet.
4) Requires Less Training – Cloud computing takes fewer people to do more work. So there is requirement of minimum training of hardware, software problems to user.

VI. SECURITY PROBLEM

The key element of the cloud computing for information technology is security. Because now these days hackers and attackers are rapidly growth to address important data on the new technologies. Many companies are adopted the technology of cloud computing for the profit of industrial and commercial . but the main concern about these companies is the security of their data.

A. Problems of Security in the Cloud

In this study we classify security problems are categorized into four type- Data ,Logical,Physical and Administrative security.
There are several risks are show which threatened the security of the stored data in the cloud by different researchers.
In the paper considered that security plays a very important role in cloud computing. They cited some problems such as security the loss of data and the problem of piracy; if hackers use the cloud services, data storage security on a hard disk of another person, they would offer free or at a cheaper price to fulfill their attacks[7].and the various security challenges in cloud computing. They discussed the protection of data and that these data should be refer to the integrity, confidentiality and availability. They also identified problems of user accessing data,with the help of IPSec (IP Security), SSL (Secure Socket Layer),secured the location and transmission of data.but there are some problems are occurred during to the

978-93-85670-72-5 © 2016 (RTCSIT)
CONFERENCE PAPER
International Conference on
Recent Trends in Computer Science & Information Technology (RTCSIT-2016)
21st August 2016
Guru Nanak College Budhlada, Punjab India

high traffic of data such as the speed and complexity of the input encoding[8].Their work showed various security issues, separating element by element. They began with problems related to data security from unauthorized access to data sources in an enterprise because the data is spread across different systems and they can be accessed by unauthorized persons[9].The traditional approach of security (explicit), whose data are stored on a single server and access to these data by a password, which is generally simple and memorable for most users, facilitated the attacks and intrusions on these data sources[10].Security of the data warehouses stored in the cloud. They showed that reliance on providers is difficult to build with the traditional architecture of the cloud based on a single provider. This architecture threatens the confidentiality of customer data since they are hosted by a single provider of external risk operate[11]

B. Problems of logic security

Logic security is a major problem in cloud computing.because it is communicated with the virtual machine.The virtualization is one of the main components of a cloud. But this poses major security risks ensuring that different instances running on the same physical machine are isolated from each other is a major task of virtualization which is not met completely into day's scenario. The other issue is the control of administrator on host and guest operating systems. Current VMMs (Virtual Machine Monitor) does not offer perfect isolation. Some vulnerabilit y has been found in all virtualization software which can be exploited by malicious and local users to bypass certain security restrictions or gain rivileges[12]. the risk of intrusion that threatens the cloud. They connects the severity of intrusions on virtual machines by factors such as the security requirements of the hosted application, the state of Service Level Agreement, the response time and the frequency of attacks on political of security[13].Virtual machines (VMs) that are managed by hypervisor in order to provide virtual memory as well as CPU (central processing unit) scheduling Policies to virtual machines. As the main source of hypervisor is managing a virtualized cloud platform, hackers are targeting it to access the virtual machine and the physical hardware, because hypervisor Resides Between virtual machine and hardware so attack on hypervisor can damage the VMs and hardware. In addition, co-location of multiple virtual machines increases the attack area and risk of virtual machine to compromised virtual machine. Intrusion detection and prevention systems must be able to detect malicious activity at the level of virtual machines, regardless of the location of the virtual machine virtualized cloud within the environment.

C. Problems of administrative security

We mean by administrative problems all cases that affect the type of provider and the type of contract. There are certain authors who have spoken on this kind of problems. According to the Padia and Parekh there may be a case that some cloud providers are not the authorized provider. They may be duplication of a Web page that already exists in order to trick and entice users into giving private or financial particulars or their passwords.

Finally, we summarized the problems that threaten the security of cloud computing on an unauthorized access to stored data, the risk of intrusion, loss of data, lack of trust between customer and supplier concern at confidentiality and availability of stored data, the poor use of services provided by malicious people, attacks on virtual machines and the type of provider and conditions of the signed contract.

V. CONCLUSION AND FUTURE WORK

In this paper, Define the overview of cloud computing and its area became used from individual instituted and defined the several threats tire protection of cloud and several risks and hacker related security problems .Cloud different risks trust between the user and the provider including loss of data, poor use of services, unauthorized access, different hardware and hacker attackes and intrusion .As we mentioned earlier, the cloud has several security problems among accessible by anyone" who exposes the cloud to several threats such as unauthorized access to data sources, data theft and intrusions. In the future, we propose a solution to control the security user access to data sources stored in the private cloud .

REFERENCES

[1] http://en.wikipedia.org/wiki/Biometrics

[2] P. Senthil, N. Boopal and R.Vanathi, "Improving the Security of Cloud Computing using Trusted Computing Technology," International Journal of Modern Engineering Research (IJMER), ISSN: 2249-6645, Volume-2, Issue-1, Jan-Feb 2012, pp-320-325.

[3] Ganesh V. Gujar, Shubhangi Sapkal and Mahesh V. Korade, "STEP-2 User Authentication for Cloud Computing," International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, Volume-2, Issue-10, April 2013.

[4] "The NIST Definition of Cloud Computing". National Institute of Science and Technology.

[5] R. Kalaichelvi Chandrahasan, S Shanmuga Priya and Dr. L. Arockiam, "Research Challenges and Security Issues in Cloud Computing," International Journal of Computational Intelligence and Information Security, Volume-3, No-3, March 2012.

[6] Nils Gruschka and Meiko Jensen, "Attack Surfaces: A Taxonomy for Attacks on Cloud Services," Proceedings of the IEEE 3rd International conference on Cloud Computing, 2010, PP-276-279.

[7] S.O. Kuyoro, F. Ibikunle, and O. Awodele,"Cloud Computing Security Issues and Challenges," *International*

Journal of Computer Networks, vol. 3,issue 5, pp. 247-255,2011.

[8] R. Maheshwari and S. Pathak, "A Proposed Secure Framework for Safe Data Transmission, in Private Cloud," *International Journal of Recent Technology and Engineering*,vol.1, issue 1, pp.78-82, April 12.

[9] N. Padia and M. Parekh, "Cloud Computing Security Issues, in Enterprise Architecture and Its solutions," *International Journal of Computer Application*, vol.2, issue 1, pp. 149-155,December 2011.

[10] A.Parakh and S. Kak, "Online data storage using implicit security,"*Information Sciences*, vol.179,pp.3323-3331, 24 May2009.

[11] K. Karkouda, N. Harbi, J. Darmont, and G. Gavin, "Confidentialité et disponibilté desdonnéesentreposéesdans les nuages," in *Proc. 9ème atelier Fouille de données complexes (FDC 12)*,pp. 1-14,2012.

[12] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, pp. 1–11, 2011.

[13]J. Arshad, P. Townend, and J. Xu, *A Novel Intrusion Severity AnalysisApproach for Clouds*, School of Computing, University of Leeds,Leeds, LS2 9JT, UK, pp. 1-13, 2011.

[14] M. Adib Bamiah and S. Nawaz Brohi, "Seven Deadly Threats and Vulnerabilities in Cloud computing," *International Journal of Advanced Engineering Sciences and Technologies*, vol. 09,
pp.087-090, 2011

978-93-85670-72-5 © 2016 (RTCSIT)

CONFERENCE PAPER
International Conference on
Recent Trends in Computer Science & Information Technology (RTCSIT-2016)
21st August 2016
Guru Nanak College Budhlada, Punjab India