IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 19-23
www.iosrjournals.org

Cloud Computing Challenges & Related Security Issues

Sabah Naseem[1] , Prof. Ashish B. Sasankar[2]
[1]*Institute of Science, NagpurR.T. Road, Civil Lines, Nagpur-440001(Maharashtra*
[2]*G. H. Raisoni College of Information Technology, NagpurHingna, Nagpur-440001(Maharashtra*
snaseem19@gmail.com,*ashish_sasankar@yahoo.com*

ABSTRACT*: The field of cloud computing has reached to the new heights of technical Developmentand also speeding up the growth of thecomputational services in organization. Evenafter transferring to the cloud becoming analluring trend from a financial approach, thereare several other aspects that must be takeninto consideration by all organization beforethey decide to implement cloud services. Thecloud services are used as and when requiredfor the users. With the tremendous growth inthe cloud environment there are major issuesthat everyone should take into considerationlike data security and protection against access control! . Because of this many organization are moving towards the cloud. There isnumber of threats which cause possible harm or used to exploit important data. A threat can be either intentional or accidental. Risk is estimated based on statistical assumptions, and those are changing overtime. There is no absolute security. In this paper we present security issues in context of the data issue & security issue provided by cloud services. The aim of this paper is to provide a better understanding of the security issues& risks in in different services provided by cloud computing.*
Keywords*: Cloud computing, cloud computing services, security issue.*

I.INTRODUCTION:

The cloud computing is the fastest growing industry. It is the advance technology where data, hardware & software are shared over a virtual network and shares resources at low cost. Cloud computing can meant different things to different people, and obviously the privacy and security concerns will differ between a consumer using a public cloud application, a medium-sized enterprise using a customized suite of business applications on a cloud platform, and a government agency with a private cloud for internal database sharing (Whitten, 2010). The shift of each category of user to cloud systems brings a different package of benefits and risks.[1] In simple words, Cloud Computing is the combination of a technology, platform that provides hosting and storage service on the Internet [2][5]. Main goal of the cloud computing is to provide scalable andinexpensive on-demand computing infrastructures with good quality of service levels [3][4][5].

II.SECURITY IN CLOUD COMPUTING:

If we wish to enable cloud computing growth and originality through security, we must have to know about security. Security has been notoriously hard to define in the general case (Avizienis et al, 2003). The information security is Confidentiality, Integrity, and Availability. We borrow from NIST to include Accountability and Assurance, and then add a sixth category of Resilience. We will discuss it below.

Confidentiality: Internal secrets and sensitive personal data be safeguarded, but metadata and transactional data can also leak important details about organization or user. It keeps data private.

Integrity: In cloud computing integrity protected against accidental or intentional modification without authorization.

Availability: Cloud providers assure customers that they will have regular and predictable access to their data and applications.

Accountability: Accountability is supported by strong identity, authentication and access control, as well as the ability to monitor transactions.

Assurance: It refers to the need for a system to behave as expected. In the cloud context, it is important that the cloud provider provides what the client has specified. Assurance is supported by a

trusted computing architecture in the cloud, and a by careful processes mapping from business case to technical details to legal agreements.[1]

Resilience: in a system allows it to cope with security threats, rather than failing critically. Cloud technology can increase resilience, with a broader base, backup data and systems, and the potential identify threats and dynamically counteract.[1]

III. CLOUD COMPUTING SECURITY ISSUES

In cloud computing security issue there are more discussion to do something for it. The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud.This leads to affects many customers who are sharing the infected cloud [7]. There are threetypes of issues raise while discussing security of a cloud.

1. Data Issues
2. Security issues

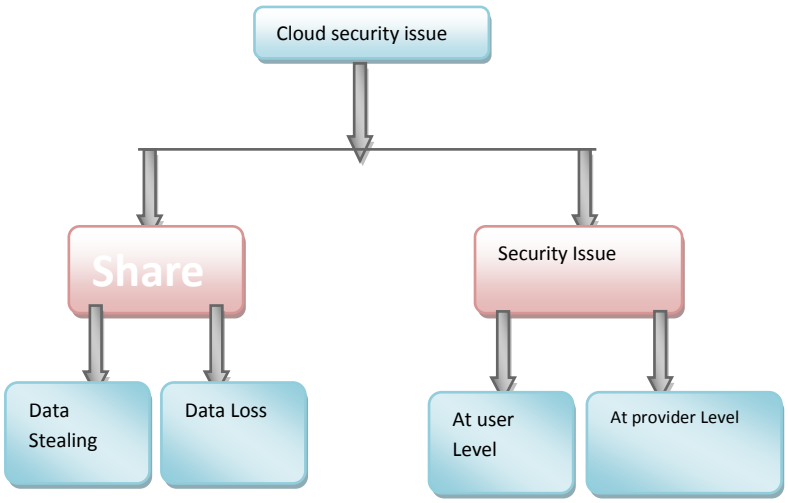

Fig-1: Cloud computing security issues

Data Issue:

Cloud computing is a virtual network. Cloud computing is based on user & provider. Provider shares all the data over a network for user. That's why anyone from anywhere can access the data easily. Sensitive data in a cloud computing environment appear as major issues with regard to security in a cloud based system.

Data Stealing:

Data stealing is a one of serious issue in a cloud computingenvironment. Many cloud service provider do not provide their own server instead they acquire server from other service providers due to it is cost affective and flexible foroperation and cloud provider. So there is a more chances that data can be stolen from the external server[7].

Data Loss:

Data loss is a common problem in cloud computing. If the cloud computing service provider shut down his services due some financial or legal problem then there will be a loss of data for the user.

Moreover, data can be lost or damage or corrupted due to miss happening, natural disaster, and fire. Due to above condition, data may not beaccesses able to users[7].

Security Issue:

In cloud computing environment the security must be from both the sides. One is from user side & other from provider side.Cloud computing service provider should make sure that the server is well secured from all the external threats it may come across. Even though thecloud computing service provider has provided a good security layer for the customer and user, the user should make sure that there should not be any loss of data or stealing or tampering of data for other users who are using the same cloud due to its action. A cloud is good only when there is a good security provided by the service provider to the user[7].

1.1) Threats affecting on cloud security:

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management [6].Security issues for many of these systems and technologies are applicable to cloudcomputing. For example, the network that interconnects the systems in a cloud has to be secure.Furthermore, virtualization paradigm in cloud computing results in several securityconcerns. For example, mapping the virtual machines to the physical machines has to becarried out securely. Data security involves encrypting the data as well as ensuring thatappropriate policies are enforced for data sharing.[7]

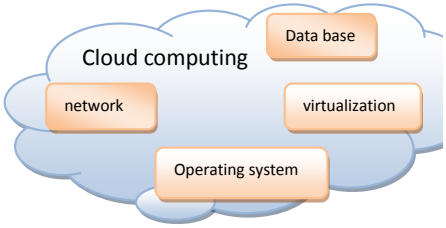

Fig-2: Threats effect on cloud

Services& Risk Level in Cloud Computing:

Cloud computing is based on different services over a network like software- as- a-service(Saas) , Platform-as-a-sservice(Paas) & Infrastructure-as –a-service(Iaas). Before starting the journey to cloud, organizations must considers the possible threats and vulnerabilities that may convert their dreams of enhancing scalability and saving management cost into a nightmare of data loss and misuse.[8]

1.1.2) Iaas(Infrastructure-as-a-service):

IaaS (Infrastructure as a Service) is a cloud computing category and a provision model in which a company outsources the physical equipment used to support operation, including storage, hardware, servers and networking components. In this model, the cloud user is usually responsible for patching and maintaining the operating systems and application software unless you are working with an Enterprise provider that offers Managed Services in their IaaS environment. Let's examine some of the risks that should be considered when evaluating Infrastructure as a Service (IaaS) solutions.

Shared resources :

One of the more obvious areas that should be evaluated with IaaS providers is performance. Cloud-based services derive their cost savings from scaling hardware and bandwidth across many different customers. In a SaaS solution, this is less critical than in an IaaS solution. For example, the bandwidth requirements for a cloud-based storage service are more demanding and require tighter tolerances than a hosted application service. One risk is that another customer monopolizes the system through large requests that leave your business suffocating for data.[9]

SLA:

Service level agreements (SLAs) in the present Cloud market are also one of the obstacles that the consumers face while adopting the services offered by the Cloud providers.Consumers might face problems that occur from vendor lock-in, insufficient security measures, data unavailability,hidden costs, and non-transparent infrastructure. In most cases, SLAs are created to protect the vendors/providers and not the customers. Most of the above mentioned problems are overlooked in current SLAs offered by the Cloud providers [15].

2.1.2) Paas(Platform-as-a-service):

In Platform-as-a-service (Paas) user can easily access the hardware, software, operating system and programming language without purchasing. In cloud user can use these things on its own machine by the help of this service.According to Wikipedia, Platform as a service' (PaaS) is the delivery of a computing platform and solution stack as a service. It facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers providing all of the facilities required to support the complete life cycle of building and delivering web applications and services entirely available from the Internet—with no software downloads or installation for developers, IT managers or end-users.[10]

Vendor Lock In:

Platform as a Service (PaaS) vendors tend to dictate the database, storage and application framework used, so what about those legacy applications? Enterprises will still require the skills and infrastructure to be able to run them. [11]

Technical Immaturity:

Every cloud framework has its own interface methods, services, and costs. The unfolding nature of the platform-as-a-service approach puts everything at risk costs could change overnight, services could be dropped, and quality of service could get worse.[12]

Privacy and Control:

Vendors generally offer extensive protection methods, and it's in theirinterests to offer high levels of security. PaaS often provides a relatively sophisticated suite ofaccess controls. But you, not the vendor, still own the risk.[12]

3.1.2) Saas(Software-as-a-service):

In the SaaS(Software-as-a-service) model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. The cloud users do not manage the cloud infrastructure and platform on which the application is running. This eliminates the need to install and run the application on the cloud user's own computers simplifying maintenance and support.[13].Risk related to Saas are as follows.

Secure data transfer.

According to (Jeff Beckham | May 3, 2011) all of the traffic travelling between your network and whatever service you're accessing in the cloud must traverse the Internet. Make sure your data is always travelling on a secure channel; only connect your browser to the provider via a URL that begins with "https." Also, your data should always be encrypted and authenticated using industry standard protocols, such as IPsec (Internet Protocol Security), that have been developed specifically for protecting Internet traffic.

Secure stored data.

According to **(**Jeff Beckham | May 3, 2011**)** your data should be securely encrypted when it's on the provider's servers and while it's in use by the cloud service. In Q&A: Demystifying Cloud Security, Forrester warns that few cloud providers assure protection for data being used within the application or for disposing of your data. Ask potential cloud providers how they secure your data not only when it's in transit but also when it's on their servers and accessed by the cloud-based applications. Find out, too, if the providers securely dispose of your data, for example, by deleting the encryption key**.**

IV.CONCLUSION:

To make cloud computing more secure virtual network. It depends on both user & provider that they perform their task well defined. The largest gaps between cloud security practice and cloud-security research theory lies in the fact that the assumptions in theresearch leave out some very important differences between actual cloud security and virtual machine security. Research should be center on these gaps and differences and its removal. One of the pieces of the framework might be developing a way to monitor the cloud's management software, and another might be development of isolated processing for specific clients' applications. People's behavior can be tracked and monitored for instance whetherpeople allow the automated patching software to run, or updating anti-virus software definitions, or whether people understand how to harden their virtual machines in the cloud.

REFERENCES:

[1] Issue in technology innovation(No.3 Oct-10) Allan A. Friedman and Darrell M. West.
[2] Harjit Singh Lamba and Gurdev Singh, "Cloud Computing-Future Framework for emanagementof NGO's", IJoAT, ISSN 0976-4860, Vol 2, No 3, Department Of Computer Science, Eternal University, Baru Sahib, HP, India, July 2011.
[3] Dr. Gurdev Singh, ShanuSood, Amit Sharma, "CM- Measurement Facets for CloudPerformance", IJCA, , Lecturer, Computer science & Engineering, Eternal University, BaruSahib (India), Volume 23 No.3, June 2011.
[4] Joachim Schaper, 2010, "Cloud Services", 4th IEEE International Conference on DEST,Germany.
[5] International Journal of Computing & Business Research ISSN (Online): 2229-6166
[6] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, BhavaniThuraisingham, Securit Issues for Cloud Computing, International Journal of Information Security and Privacy, 4(2),39-51, University of Texas, USA, April-June 2010.
[7]Prince Jain, Security Issues and their Solution in Cloud Computing,International Journal of Computing & Business Research ISSN (Online): 2229-6166
[8]MervatAdibBamiah* et al. / (IJAEST) INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES AND TECHNOLOGIES Vol No. 9, Issue No. 1, 087 – 090
[9] SearchCloudSecurity.com E-Guide
[10]Google (Top 5 risk with Paas)
[11] http://en.wikipedia.org/wiki/Platform_as_a_servicehttp://www.cloudsecurityalliance.org/
[12] Dr.Dobb's (Cloud Computing Platform-as-a-service)(Oc t . 2 , 2 0 0 9)
[13]HamdaqaMohammad.*AReferenceModelforDevelopingCloudApplications*.http://www.stargroup.uwaterloo.ca/~mhamdaqa/publications/A%20REFERENCEMODELFORDEVELOPINGCLOUD%20APPLICATIONS.pdf
[14]Anthes, G..(2009, January).SaaS Realities. Computerworld, 43(1), 21-22. Retrieved August 9, 2009, from ABI/INFORM Global. (Document ID: 1626575741).
[15]SearchCIO, "Beware these risks of cloud computing, from noSLAs to vendor lock-in," Aug 6 2009.