ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICACTRP 2017

International Conference on Advances in Computational Techniques and Research Practices

Noida Institute of Engineering & Technology, Greater Noida

Vol. 6, Special Issue 2, February 2017

A Survey on Cloud Computing Security Issues

Mehak Choudhary[1], Mohit Choudhary[2], Twinkle Tyagi[3]

Assistant Professor, Department of Computer Science, NIET, Greater Noida, India [1]

Assistant Professor, Department of MCA, NIET, Greater Noida,India [2]

Assistant Professor, Department of Computer Science, NIET, Greater Noida, India [3]

Abstract: Cloud computing is a way to share resources and services over internet. It is the set of services which are being provided to the customers over network on the pay per use basis. Services of the cloud computing are provided by third party provider. SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) are several services that are provided by service providers. There are many issues such as load balancing, VMM (Virtual Machine Migration), scheduling of requests. One of the major issues in cloud computing is "security". This paper mainly focuses on the technical security issues associated with the usage of cloud services.

Keywords: Cloud Computing, Computing Computing Security, Security Threats, VMM.

I. INTRODUCTION

Cloud computing is the emerging technology that is putting forward the theme of virtualization, data storage. Cloud Computing are the internet based services where internet means collection of clouds thus cloud computing is defined as the use of internet to provide technology related services to people and organization. Resources can be accessed by consumers online through internet, from anywhere at any time without the issues based on technology and physical management. One of the example of cloud computing are Google Apps through which services can be accessed through browser and deployed on millions of machines over internet. Cloud can also be defined as "On demand IT" or utility computing. Cloud is concerned with storage and data accessibility through internet of using computer's hard drive. Cloud Computing are categorized on the basis of two ways: 1.On the basis of services provided.2.On the basis of locality.

On the basis of services provided Cloud Computing are categorized in three ways:
1. SaaS (Software as a Service) which provides software as services according to their need, here client can use services that are hosted on cloud server.SaaS takes away the organization's need to installation handling, setting and maintaining. Example of SaaS solution is Google+, gmail. Common and popular example of CRM (Customer Relationship Management) SaaS application is Salesforce.
2. PaaS (Platform as Services) provide platform access to clients that enables client to put their customized software and applications on cloud.PaaS supports the facilities of application development, application deployment, testing and also supports hosting of web applications. Programming languages and development environment are supported by it. Example of PaaS is Microsoft Azure and Heroku.
3. IaaS (Infrastructure as Services) provides storage, network capacity and other basic computing resources. IaaS provides hardware related services using principle of Cloud Computing. It is phenomenon of on demand services of cloud computing. IaaS providers provide space for virtual datacenters and all the utilities to maintain cloud server and storage. Example of IaaS is Amazon and VMware.

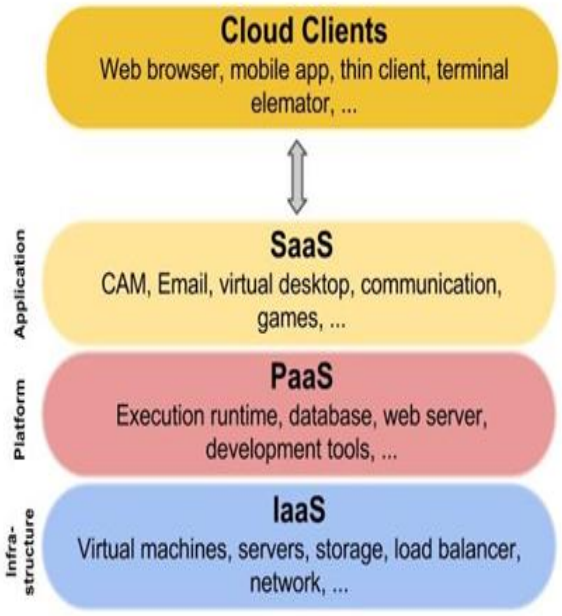

Fig.1. Example of an unacceptable low-resolution image

On the basis of locality it is further divided into four types.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICACTRP 2017

International Conference on Advances in Computational Techniques and Research Practices

Noida Institute of Engineering & Technology, Greater Noida

Vol. 6, Special Issue 2, February 2017

1.Public Cloud: Public Cloud are available to large organizations that are owned by third party organization that offers cloud servers.
2. Private Cloud: Private Cloud is used for specific group or organization and for limited access to that group private cloud is used. It is also called "internal cloud".
3. Hybrid Cloud: Composition of two or more cloud models is called hybrid. There are two methods to offer hybrid cloud: either having private cloud vendor partnership with public cloud provider and viceversa.
4. Community Cloud: Community Cloud lies between private and public clouds with respect to target set of consumers. Objective of community cloud is to have benefits of public cloud that is shared infrastructure costs and pay as you go billing structure with added private cloud's benefits of security and privacy.
There are number of issues related with security of cloud computing as it deals with many technologies including network,database,virtualization,scheduling.The issue related with security in virtualization are mapping of virtual machine's to physical machines are to be done carefully. Encryption of data that is involved for data security.

II. CLOUD COMPUTING SECURITY CHALLENGES

There are some security issues that are related with cloud delivery models and deployment models. Few of them are discussed below:

A. Identification and Authentication

In Cloud Computing, there must be access to priorities and permissions depending upon the type of cloud and delivery models. Process focused on verification and validation of cloud users through usernames and passwords protections from the cloud profile.

B. Authorization

Authorization is a mechanism to maintain the referential integrity. Through this control and privileges are provided with cloud computing. System administration maintains authorization in private cloud.

C. Confidentiality

In cloud computing, for maintaining data's control that are situated across multiple distributed databases, confidentiality is very important. Confidentiality protection for access control can be done through identity management, end-to-end confidentiality and integrity assurance.

D. Confidentiality

In cloud computing For maintaining integrity within the cloud domain while accessing data ACID (atomicity, consistency, isolation and durability) properties should be maintained across all cloud computing delivery models.

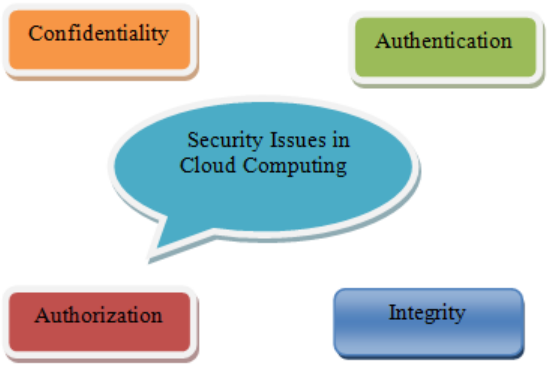

Fig.2. Example of an unacceptable low-resolution image

In terms of database data integrity, refers to the process of ensuring that the database reflected accurately as it is modeled or represented.

E. Non-Repudiation

Repudiate means to deny. Non-Repudiation is the ability for ensuring that a party that is communicating can't deny the authenticity of their signature on document or sending message that they originated. It can be maintained through digital signature, time stamps and confirmation receipt services (digital receipting of messages confirming data sent/received).

F. Data Loss

Data loss is the process where data gets currupted, deleted or made unreadable by user, software. Data loss can also be termed as Data Leakage. Data loss can occur in both data at rest or in motion. Hacker, spyware and inadvertent data breaches can also lead to data leakage from company server. Many algorithms are developed to maintain data leakage.

G. Privacy Issues

In cloud computing personal information security is very important. Protection of personal information (or data protection) derives from the right to privacy.

H. Security Issues in Providers level

There should be a good security level between maintained between service provider and client. Provider should maintain a good security between customer and user. There must be a SLA (Service Level Agreement) between user and provider that security level.

I. Data Access Control

Lack of Data Access Control can cause loss of confidentiality of data that are accessed illegally. Sensitive data plays a very important role regarding security in Cloud Based System.The template is designed so that author affiliations are not repeated each time for multiple authors of the same affiliation. Please keep your affiliations as succinct as possible (for example, do not

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICACTRP 2017

International Conference on Advances in Computational Techniques and Research Practices

Noida Institute of Engineering & Technology, Greater Noida

Vol. 6, Special Issue 2, February 2017

differentiate among departments of the same organization). This template was designed for two affiliations.

III. SECURITY ISSUES IN SERVICE MODELS

A. Security in SAAS

There are number of security issues that are associated with SaaS such as security of data, network security, and locality of data, integrity authentication and confidentiality of data. Virtualization vulnerabilities and authorization of data.

B. Security in IAAS

In this model the focus in to manage virtual machines because there can be uncontrolled access and wastage of cost. Thus the vulnerabilities not only associated with web applications but also associated with machine to machine. Data leakage protection, authentication and authorization are some issues associated with IaaS.

C. Security in PAAS

PaaS allows organizations to build, run and manage web applications without the infrastructure. It also provides dynamic load balancing capacity across multiple file systems and machines. Here security issues are related with data and balancing the load.

IV. SOLUTION FOR CLOUD SECURITY ISSUES

As we have seen there are many cloud security issues present in Cloud Computing, there are few solutions that are very helpful for securing cloud from threats.

A. Examine Support

When data is stored by users in cloud they don't have information where the data is stored. Therefore Cloud Service Provider must provide auditing tools to the users to examine and regulate how the data is stored, protected, used and verified. But examining of illegal activities is a difficult task. Thus data for multiple users may be collocated. For this audit tools are used.

B. Recovery Facility

Cloud Providers must provide safe and helpful recovery facility, so that in any situation if data is lost because of any reasons, data can be recovered.

C. Encryption Algorithm

Cloud Service Provider encrypts user's data using strong encryption technique but in some circumstances encryption can make data completely useless and on the other side encryption also complicates the availability of data. To solve this issue technique were design and tested properly.

V. LITERATURE REVIEW

Bhaskar Prasad Rimal et al.[1] stated the survey on cloud computing and taxonomy related to cloud computing .Cloud Computing is most commonly used technology in this era which process large scale of data. For example Google process 20 terabyte of webdata.In taxonomy cloud computing, cloud architecture is discussed which has layered architecture of demand services and these services can be accessed anywhere. Services are IaaS,PaaS,SaaS and HaaS.On the basis of location cloud is categorize into four categories public cloud, private cloud, hybrid cloud and community cloud.

Yashpalsingh Jadeja et al. [2] discussed the concept of cloud computing and architecture. Earlier the concept of parallel computing and distributed computing was used commonly, after that grid computing came into existence and now cloud computing is recent trend in IT. Cloud computing uses the concept of virtualization, interoperatability and quality of services. It uses the facility of pay-per-use of application per client. Paper also discussed the architecture of cloud that comprises of two parts front end and back end where front end is client and backend is internet.

Rongxing et al. [3] discussed the security proposals in cloud computing. Proposed system provided privacy and security on the documents and files that are present in cloud. Authentication mechanism is also proposed for controlling unauthorized user access. It has a limitation that it is difficult to implement complex mathematical model.

Soren et al. [4] discussed the advantages of cloud that include security, safety and privacy due to which adoption of cloud computing is inhibited. This paper discussed an approach that is used to analyze security at both ends that is at client and server both ends. It primarily focused on accessibility, vulnerabilities in cloud. Special query policies for accessment have been proposed in this paper. Python is used for implementation.

S Ramgovind et al. [5] discussed the needs of security in cloud. Paper provided the security perspective of Cloud Computing which aims for security concerns that should be properly addressed and managed to realize the full potential of cloud computing. Few security issues are highlighted by authors that are 1.Privileged Access 2. Recovery 3.Data Availability.

Jiang chun Ren et al. [6] proposed a framework ESI (Easy Security Services Integration Cloud) for managing the security services in cloud computing platform. It also introduces the concept of Virtual Machine's introspection that monitor and analyze the guest Virtual Machine's execution information.ESI cloud implementation is done in Xen hypervisor platform and system functionality and performance are evaluated.

Mohammad Alhamad et al. [7] presents the design in cloud computing. Here the strategies between cloud

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICACTRP 2017

International Conference on Advances in Computational Techniques and Research Practices

Noida Institute of Engineering & Technology, Greater Noida

Vol. 6, Special Issue 2, February 2017

provider and cloud consumer are discussed. This paper proposed the method for the maintenance of trust and reliability. The main contribution of paper is to analyze the SLA (Service Level Agreement) metrics for users. The metrics in IaaS are CPU utility, security, usability etc.In future SLA metrics are required to be designed and should be implemented for testing the framework in cloud computing. Paper also discusses the strategies of negotiation between cloud provider and consumer/client. First criteria include direct migration that is done online. Second criteria include negotiation via trusted system. Third criteria include more than one system for negotiation.

VI. CONCLUSION AND FUTURE WORK

Security and privacy related research are briefly studied in this study.Although cloud computing have many advantages but it has a constraint of security threats. There should be mutual understanding between service provider and client for ensuring the security and safety of cloud. Approach related to Security analysis and risk analysis will help service providers for ensuring consumer about security of data. This paper focused on the security consideration and challenges which are occurring in cloud computing. Data loss, privacy, user's authentication, malicious users handling are few security concerns of cloud computing. Future work should be done towards cloud computing security protocols.

REFERENCES

[1] Bhaskar Prasad Rimal, Eunmi Choic and Ian Lumb," A Taxonomy and Survey of Cloud Computing", IEEE, pp.44-51,2009.
[2] Yashpalsingh Jadeja and Kirit Mali," Cloud Computing-Concepts, Architecture and Challenges",IEEE,pp.877-880,2012.
[3] Rongxing Lu, Xiaodong Lin,Xiohui Liang and Xuemin Shen," Secure Provenance: The Essential Bread and Butter of Data Forensics in Cloud Computing" ASICCS
[4] Soren Bleikertz,Matthias Schunter,ChristianW.Probst,Dimitrios Pendarakis and Konrad Erikson,"Security Audits of Multi-Tier Virtual Infrastructure in Public Infrastructure Clouds",CCSW,2010.
[5] S Ramgovind,MM Eloff and E Smith,"The management of Security in Cloud Computing",IEEE,August 2010.
[6] Jiang chun Ren,Ling Liu,Da Zhang,Huaizhe Zhou,QiZhang,"ESI-Cloud:Extending Virtual Machine Introspection for Integrating Multiple Security Services", IEEE, July 2016.
[7] Mohammad Alhamad, Tharam Dhillon and Elizabeth Chang," Conceptual SLA framework for Cloud Computing", IEEE, 2010.
[8] http://lfu.edu.krd/item/issue03/issue_Cloud_Computing.php