Volume 4, Issue 5, May 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Cloud Systems Security Threats And Prevention Mechanisms

Nikunj Kumar* CSE,UPTU
Prof. Priti Sharma CSE,Amity University

Abstract --- Cloud computing is a model for enabling service, on-demand network access, that's why cloud computing become the buzzword in the IT industry. The Possible Threats at various ends for Cloud Computing is emerging area for study and this paper provide security threats,its description and organised Prevention in terms of cloud computing based on analysis of Cloud Security threats and also embedded the risk assessment index.
As per time passes,have revealed new security issues. This research paper revealed an analysis of the existing status on cloud computing security issues based on a detailed survey carried by the author.

Keywords: Cloud Computing, Security threats for user and provider, Risk Assessment Index

I. INTRODUCTION

Cloud computing is a service model for enabling user's on-demand network access to a shared pool of computing resources (storage, applications, services etc), that can be instanteanously released with certain effort and service provider interaction. Cloud computing enables cloud services[1].

The security architecture and functions highly depend on the architecture, and this paper shows the architecture and the main security issues and preventions concerning this architecture from a cloud computing user's end and cloud computing provider's end, cloud computing provides a means for acquiring computing services without any need for deep understanding of the underlying technology being used. From an organizational scenario, cloud computing delivers services for consumer and has four different deployment models namely private model, community model, public model and hybrid model as well as three different delivery models that are utilized within a particular deployment model. These delivery models are the SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service). These models exhibit key characteristics like on demand self-service, broad network access, resource pooling etc.
As shown in the FIG-1, key functions of a cloud management system is divided into five layers, respectively the Resources & Network Layer, Services Layer, Access Layer, and User Layer[2]. Each layer includes a set of functions:

1) The User Layer describes the various functions of End-user, Partner and Administration
2) The Access Layer describes API termination function and Inter-Cloud peering.
3) The Services Layer describes the categories of cloud services, the service automated arrangement function and the cloud operational function.
4) The Network Layer manages the physical and virtual resources.
5) The Cross Layer includes Other functions like Management, Security & Privacy, etc.

TABLE-I

USER LAYER
ACCESS LAYER
SERVICE LAYER
NETWORK LAYER
CROSS LAYER

II. LITERATURE REVIEW

- **"Security Framework For Cloud Computing Environment:A Review (2012)"[3]** describes the need of IT companies and infact it is very adventages to them ,thinking to take serious concern regarding to review their

existing security challenges and threats. If they review these threats in time bound manner,yhey became very beneficial and successful solution of these critical problems.

This paper is basically focuses on various characterstics, models and various aspects of cloud computing and also gave gist of seven-eight papers related to same sector. It is also associated with various attacks in certain channels in cloud computing and provide the solutions basis of API or server side access control also.

- **"Security Threats In Cloud Computing Environment (2012)"[4]** describes as the cloud computing service is a on-demand service and provides the network access in certain pooled resources. It basically analysis of cloud computing threats and technically components of cloud computing. It envisages the various layers of computing the specific clouds and describes the inter/intra related functions between them. It also included the threats for cloud computing and cloud computing users and also collectively comprises threats for cloud computing services providers also.
- **"Securing Software As A Service Model Of Cloud Computing: Issue And Solutions(2013)"[5]** describes that the impact of cloud computing basically affected not only bussiness life but also our day to day life also. Disruptive technology used is very injurious to business as well as for existing security system also. This paper deals with existing strategies of cloud computing security based upon large viewed survey and try to overcome the existing problems and challenges in SaaS model of cloud computing with some futuristic security research directions.
- **"The Notorious Nine Cloud Computing Top Threats(2013)"[6]** describes the recent cloud computing threats affecting to IT campanies and organisation on large scale on widespread. In this paper it covers how to recognize the threat in your organisation ,what is the implications of this in existing system or technology , what remedy used aganist it to overcome and what types of links exists between these service threats to other in efficient, economical and productive way.
- **"Top Cloud Security Threats (2014)"[7]** describes the current perception of private,public and hybrid cloud in intensive cloud computing. How cloud computing services included health sector,education sector,diaster management,e-commerce,data storage etc in very minimal cost, time bound manner and productive manner, this paper also put the light on various types of cloud computing systems available in the market and what type of flexibility,elasticity provided with effectiveness involving cloud computing. It also comprises animals threats in cloud computing and gives the solution to resolve them.

III. PROBLEM STATEMENTS AND PREVENTION

Our reasearch focus is to provide the solution for those threats which is frequently arises in Cloud Service Users,Cloud Service Providers and as a Security attacks exhibit in specially SaaS(Security as a Service).[8]

For this purpose, a prototype should be designed for execution of data and information securely in cloud environment. It will protect users' data and information against various attacks.

This research comprises to study the major threats occuring in cloud environment, technologies used and problems that still there.

(a) Threats For Cloud Service User

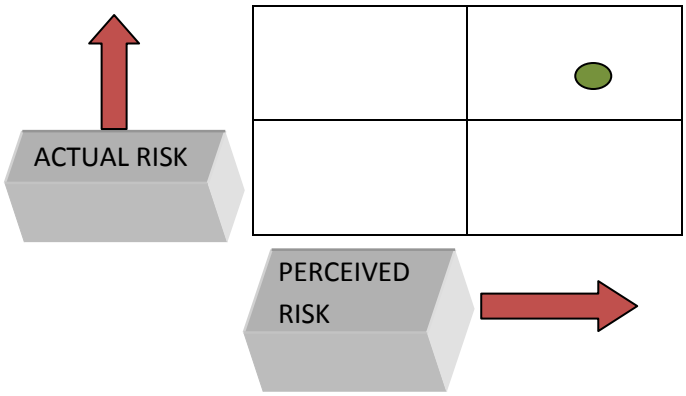
Threats	Discription	Available Prevention
Accountablity Ambiguity	The lack of a clear definition of accountability among cloud service users and Providers may evoke conceptual conflicts.	Install data controller in which the data processor measure conflict on scale
Loss of Mutual Inclusion	It is difficult for a cloud service user to recognize his provider's trust level due to the black-box feature of the cloud service.	To evaluate security implementation level achieved by the provider.
Data Leakage	The loss of encryption key or privileged access code will bring serious problems to the cloud service users.	Encryption keys, authentication codes and access privilege was heavily lead sensitive damages on data leakage[9]
Lack of Asset Management	location of sensitive asset/information, lack of physical control for data storage, reliability of data backup (data retention issues)	Reliability of data backup, counter measures and Disaster Recovery etc.
Unsecure User Access	Attack methods such as phishing, fraud of software vulnerabilities still achieve results. Reusing the credentials and passwords.	Authentication codes, Encryption keys with PKI in cryptographic approach.

(b). Threats For Cloud Service Providers

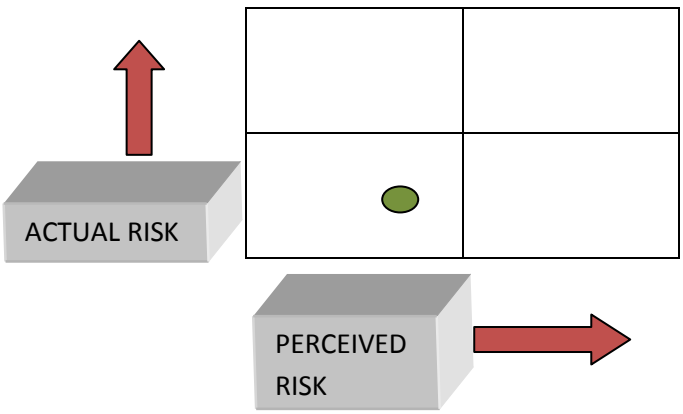
Threats	Discription	Available Prevention
Protection Inconsistency	Due to the decentralized architecture of a cloud infrastructure, its protection mechanisms are likely to be inconsistency among distributed security modules.	To provide confidentiality and integrity.
Risks of Evolution	Some dependent software components of a system may be selected and implemented when the system executes.	Conventional risk assessment methodology to mitigate the risks of Evolution
License Risks	The lack of a "clouded" license management scheme which allows to pay only for used licenses may cause software use conflicts.	Created virtual machines and adopted "clouded" license management scheme.
Bad Integration	A bad integration caused by incompatible interfaces or inconsistent policy enforcement may evoke both functional and non-functional impacts.	Moving large amounts of data and major configuration changes[10] (e.g. network addressing)
Shared Environment	Any unauthorized and violent access to cloud service user's sensitive data may compromise both the integrity and confidentiality.	Cloud resources are virtualized, architecture compartmentalization etc
Service Unavailablity	The dynamic dependency of cloud computing offers much more possibilities for an attacker. A attack on one service may clog the whole cloud system.	The service-oriented design principle, service delivery aspects etc.

(c). Risk Analysis Of Cloud Service Therats[11]

- **Massive Cloud Therats Risk Index**



- **Lower Cloud Therats Risk Index**



IV. Different techniques used for protection of cloud computing

- **Privacy Manager[12]** It is used as the alternative remedial apporach for cloud threats at user's end It helps to reduce the threat of data leakage and loss of private data that processed in the cloud, as well as provides additional privacy related benefits.
- **Cloud Protection System** It is used as the alternative remedial apporach for cloud threats at user's end in asset management This is a protection system for clouds designed at clearly monitoring the reliability of cloud components.CPS is planned to protect the integrity of distributed computing by allowing the cloud to monitor infrastructure components.
- **Efficient Access to Outsourced Data** Providing secure and efficient access to outsourced data is an important factor of cloud computing and forms the foundation for information management and other operations.

IV. CONCLUSION

Cloud computing is boon for IT sector whether it is used in efficient and effective way.Despite knowing its advantages like no further dependency over server,cost effective ,time saver,no inadequate manpower required, It also embedded the certain threats and risks, Basically in this research paper included all possible those threats which occured during the processing on user's end and supplier's end. How it mitigated? What is the suitable remedies available in world ,properly and organised manner it discussed. A risk assessment technique is also used for better understanding the massive and lower cloud threats risks.

In this paper an overview of cloud computing,possible threats at both the ends with clear understanding and descriptions and available proper prevention.

REFERENCES

[1] IEEE CCSSG. IEEE Cloud Computing Standard Study Group http://www.computer.org/portal/web/sab/cloud.[Accessed : January 2013]

[2] SNIA.(2013).Storage Networking Industry Association. http://www.snia.org/ .[Accessed : January 2013]

[3] Security Framework for Cloud Computing Environment: A Review, ISSN 2079-8407 VOL. 3, NO. 3, March 2012

[4] Security Threats in Cloud Computing Environments, International Journal of Security and Its Applications Vol. 6, No. 4, October, 2012

[5] Securing Software as a Service Model of Cloud Computing: Issues and Solutions International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol.3, No.4, August 2013

[6] The Notorious Nine Cloud Computing Top Threats in 2013,Feb-2013,cloud security allience,

[7] Top Cloud Security Threats, JANUARY 28, 2014 BY GILAD PARRANNISSANY Top Cloud Security Threats - Porticor Cloud Security

[8] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, https://cloudsecurityalliance.org/research/security-guidance/, (2011) November.

[9] Agentless Recovery.(2013).http://www.ibm.com/developerworks/cloud/library/cl-agentlessrecovery/[Accessed : January 2013]

[10] D. Xu, Y. Li, M. Chiang and A. R. Calderbank, "Elastic Service Availability: Utility Framework and Optimal Provisioning", IEEE Journal on Selected Areas in Communications, vol. 26, no. 6, (2008) August.

[11] Cloud Security Alliance. Guidance for identity & access management V2.1,2010 <http://www.cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf> [Accessed :July 2012].

[12] Pratap Murukutla, K.C. Shet (2012).Single Sign On for Cloud .In: International Conference on Computing Sciences,2012 IEEE DOI 10.1109/ICCS.2012.66

