IJCAT - International Journal of Computing and Technology, Volume 3, Issue 11, November 2016
ISSN: 2348 - 6090
www.IJCAT.org

A Comparative Analysis on Categorization of Different Threats in Cloud Computing Environment

[1] Arati Koli, [2] Dr. Nilesh Uke , [3] Dr. Swati Shinde

[1] M.E. Student, Dept. of IT, Pimpari Cinchwad College of Engineering, Pune, India

[2,3] Professor, Dept. of IT, Pimpari Cinchwad College of Engineering, Pune, India

Abstract - The cloud is emerging technology now days, but adoption of this technology includes some major concerns like hardware, virtualization, network, abuse of cloud services, challenges with data in storage as well as in transmit. Even the cloud provides many advantages like reduction in cost by providing different scalable and highly flexible services such as Infrastructure as a Service (IaaS), Software as a Service (SaaS), Platform as a Service (PaaS) the cloud consumers always afraid to use cloud services due to the threat barriers. In this paper we survey top threats which are associated with cloud computing and categorized top threats into three categories that is internal threats, external threats and critical threats. This paper helps cloud consumers to analyze which threats are more critical and how they affect the different components of cloud.

Keywords **- Cloud Services, Virtualization, Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS), Threats.**

1. Introduction

In recent years, the cloud has become the major technology. The companies has been using its services such as Infrastructure as a service (IaaS), Software as a Service (SaaS), Platform as a Service (PaaS) ,this services provides the additional computing power and high storage capabilities which are required for constructing IT services, also provides facilities to user for hosting there software application. In daily life we are using many cloud services such as the cloud email services (e.g. yahoo, Google) for communicating through mails; some social impacts of cloud such as facebook, twitter, instagram to share pictures, audio, video among friends and helps to connect with people globally. The cloud provides file sharing services such as Google Drive, Apple iCloud, Dropbox and Box.net. The images clicked on Android Phone and uploaded on Google Drive can be accessed by many users. The video calls and TELECONFERNCING might be the most overlooked cloud based services. Facetime, Skype, GoToMeeting allow to make video calls to loved ones, friends, co- workers across country as well as globe.

Even though the cloud has numerous advantages the people are still afraid of using cloud services due to some threats associated with different entities of cloud. The threats are major barriers in adoption of cloud services, as hosting cloud means placing organizations high confidential information in third party cloud provider, so the security of such a data is major concern. Identification of such threats in cloud is challenge for cloud providers as well as for cloud consumer.

In this paper we categorized threats as external, internal and critical threats, this categorization is based on analysis of threats caused by external entities like outside hackers, attackers which are major concern to the cloud data which would be in the form of stored or processing. The category of internal threats consist of all threats which are caused by either the employees, the third party or other peoples who works as a part of organization and misuses there privileges to damage organizations information assets. The critical threats can cause serious issue if not found and tackled earlier. In the literature many people categorized the threats in different manner and with their own aspects. In [1] paper security issues in different service models are discussed and also categorized different threats based on their appearance in service models. A paper [2] discussed different security domains and the distribution of publication by threats and domains. The threats along with its countermeasures are provided in [3] paper. In paper [4] all the security threats in cloud computing environment for

year 2003 has explored and also provided different approaches to secure cloud environment. The categorizations of threats based on their appearance in different network layers are proposed in [5] paper.

2. Literature Survey

Many researchers have reviewed threats and vulnerabilities in cloud environment with different perspectives. Mostly studies aims to identify risks and serves as a source for threat recognition that will help cloud clients and vendors to settle on educated choices about risk relief inside a cloud environment.
A paper on Security Threats in cloud computing [1] discussed security issues in different service models and authors categorized threat based on their appearance in different Service models i.e. Software as a Service, Infrastructure as a Service and Platform as a Service.

In [2] the authors has discussed Security Domains and the distribution of publication by Threats and domains has shown (7threats *12 security Domains).

Authors provided useful list of threats and also categorized Threats by considering different aspects, after that listed some countermeasures [3]

In [4] the study explored all the threats and vulnerabilities associated with cloud computing technology in organization of oman. The main findings of this paper shows that the data control and privacy, security risks and security threats are major barriers in adapting cloud technology, finding and mitigating such threats are very important.

In [5] this work presents categorization of the threats based on their appearance on different layers i.e.
Network Layer, Application Layer, Session Layer.

Imperial analysis of computing is carried out by [6]. Authors in [7] discussed various existing solutions provided for dealing with security threats in cloud and provided a comparative analysis. There objective is give better understanding of the various security problems associated with the cloud, current solution space, and future research scope to deal with such attacks in better way.

3. Review of Threats in Cloud Environment

The review of threats is done by considering various parameters, such as the threat exploits internally or externally through the outsider of cloud. The category of threats are decided based on either it is critical, internal or external. All this categorization of threats in cloud environment is shown by table below which describe the different threats and category of each one based on their appearance either these are critical or not and they are exploited by inside or outside person.

3.1 Categorization of Top Threats in Cloud Environment

The cloud computing security is very topical. Threats are major barriers in the acceptance and deployment of cloud services. The top nine Threats are categorized as: data breach, Data Loss, Account Hijacking, Insecure APIs, Denial Of Service (DOS), Malicious Insider, Abuse of Cloud Service, Security Concerns with the Hypervisor, Shared Technology Issue. The nine threats are classified in major three categories as: Internal threat, External Threats and Critical threats.

The data breach, Data Loss, Account Hijacking, Malicious Insider, Abuse of Cloud Service and Security Concerns with the Hypervisor threats are categorized as a critical because existence of such threats cause serious problems to the cloud users as well as for cloud providers.

Insecure APIs threat can be easily solved by avoiding entry points to malicious outsiders while writing APIs, Some measures can be taken to mitigate the Denial Of Service (DOS) such as adding the filters to the router so that router will discard all malicious packets, set lower flood drop threshold and set timeout half-open connection. Shared Technology Issue threats could be tackled by ensuring the cloud component designs separates the data and resources belongs to different users.

Table 1-Catagorization of top threats in cloud environment

Threats	**Description**	**Internal Threats**	**External Threats**	**Critical Threats**
Data Breach	The intentional or unintentional disclosure of information, data spill.	Yes, it occurs due to inadequate physical security Procedures, rogue administrator, exploitation of cloud vulnerabilities [1].	Yes, The organization hosting data on cloud may become the victim of cyber theft.	Yes, it is critical threat if the cloud consumers became the victim of spam mail or loose there sensitive data by compromising their database password due to security breach.
Data Loss	Data is highly sensitive information security asset it can be compromised by internal employee or external hackers.	Yes, deletion of data without backup by employee.	Yes, unauthorized access by hacker to organization database.	Yes, business may Lose their reputation by compromising sensitive data hence critical.
Account Hijacking	It includes the denial-of service attack, phishing, man-in-the middle attack	No	Yes, the attacker can eavesdrop the activity of legitimate user s and alter it data and redirect it to receiver.	Yes, it can be applied to harass three layers of systems. For example, the browser to get authorized access, malicious worm, and virus can be injected to perform damage. Malicious operation embedded into the normal command.
Insecure APIs	The application programming interface is entry point to cloud services; it must have secure access control mechanisms, encryption and log audits for monitor user access.	No	Yes, the poorly written APIs may become entry point for malicious outsiders.	No
Denial Of Service(DOS)	The DOS makes service unavailable for Authorized users.	No	Yes, in this the server flooded by large service request by attacker hence, the services are unavailable to legitimate users.	No
Malicious Insider	Malicious insider threat is part of organization (i.e. employees, contractor, or any third party) that has authorized access to information assets such as network, data, and hardware.	Yes, the insider may damage the information asset by misusing his authority.	No	Yes, identifying the insider threat is very difficult task, as by having access credentials The insider may damage highly sensitive data of organization.
Abuse of Cloud Service	Abuse and nefarious use of cloud computing is the top threat identified by the Cloud Security Alliance (CSA) [3].Gain large no of attacking instances.	Yes, the any compromised insider of organization can upload the malware to computers intentionally or unintentionally.	Yes, hacker may misuse the available resources on cloud for example, the attacker may misuse the virtual machines and use as a platform for attack.	Yes, once the attacker gain attacking instances by abusing cloud services he gets complete control over cloud services.
Security Concerns with the Hypervisor	The hypervisor in virtualization allow multiple operating systems on single platform. The malicious code run on host and brings system down.		Yes, the malicious user may use guest host as attacking instance and perform serious damage.	Yes, by compromising hypervisor attacker can gain access to all machines which are running on top of hypervisor.

Shared Technology Issue	In IaaS Ensuring the separation of data and resources belongs to different user is major challenge.	Yes, possibilities that users may thread on each other's data and resources are more.	No	No

In [1] threats are categorized based on their appearance in service models such as the threats which affects PaaS, SaaS and IaaS. The threats may be classified based on their occurrences and nature into the cloud environment.
Table 1 provides the top threat categorization based on occurrences and nature of threats in cloud computing environment.

4. Conclusion

The cloud computing technology gain popularity in recent years. Even though the cloud provides many benefits to cloud consumer such as storage services, Capital-expenditure free, Flexibility, increased collaboration, Work from anywhere still cloud has some vulnerability and threats which opens security holes to attackers. In this paper, we examined and categorized threats from three perspectives (internal threats, external threats, and critical threats). In the future, we will study the countermeasures to cloud computing threats and vulnerabilities.

References

[1] SHAVETA DARGAN, ”Security threats in cloud computing environment” ,JOURNAL OF INFORMATION, KNOWLEDGE AND RESEARCH IN COMPUTER ENGINEERING,2015.

[2] Carlo Marcelo Revoredo da Silva, ”Security Threats in Cloud Computing Models: Domains and Proposals” IEEE Sixth International Conference on Cloud Computing 2013.

[3] Neha Kajal ,”Security threats in cloud computing”, International Conference on Computing, Communication and Automation (ICCCA2015).

[4] Muhammad Kazim, ”A survey on top security threats in cloud computing”(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 3, 2015.

[5] Prachi Deshpande*,”Security Threats in Cloud Computing” International Conference on Computing, Communication and Automation (ICCCA2015).

[6] Londhe, Ruchita D; Sherekar, Swati S; Thakare, V M. International Journal of Advanced Research in Computer Science5.4 (Apr 2014).

[7] Zhaolong Gou , Shingo Yamaguchi and B. B. Gupta,"Analysis of Various Security Issues and Challenges in Cloud Computing Environment: A Survey", Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, 2016.

Author Profile:

Arati Koli has obtained her degree in information technology from Pune University in 2013 with first class with distinction and now pursuing master degree with Honors in information technology. Her current research interests in data mining, cloud computing security and NoSQL databases.

Dr. Nilesh J. Uke received the BE degree in Computer Science and Engineering from Amravati University, in 1995 , ME in Computer Engineering in 2005 from Bharathi University Pune and Ph.D. in Computer Science and Engineering from SRTM University Nanded, India in 2014. He is currently working as Professor at department of Information Technology, Pimpri Chinchwad College of Engineering, Pune. He is a member of IEEE, ACM, CSI, ISTE.

Dr. Swati Shinde received her B.E. (CSE) degree from SRTM University, Nanded, M.E.(Computer) degree from Bharti Vidyapeeth Pune and Ph.D. in Computer Science and Engineering from SRTM University Nanded. She is working as a Professor in Pimpri Chichwad College of Engineering. He is a member ISTE.