Volume 6, Issue 4, April 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Study on Threatened Risks for Cloud Computing Security & How to Overcome These Risks

Md. Alam Hossain, Syeda Taslima

Department of Computer Science and Engineering, Jessore University of Science & Technology
Jessore, Bangladesh

Abstract-Cloud computing is a network based or internet based technology, which gives dynamic resource services for the customer on demands. It moves data away from desktop & PCs into large data centers. Cloud services are delivered from data centers through the world .It is a totally internet based service. It uses as a pay-per-use pattern through the network. Cloud computing is a service of 'Networks of Networks'. Third party involvements also present there. So secure architecture is important to keep Cloud computing data safe from the beginning cloud computing, it provides better service, low-cost services etc .Despite that there are several threatened risks in cloud computing, the aim of this paper is to study on "Threatened risks for cloud computing security & how to overcome those risks".

Keywords: Cloud computing, cloud security, threatened risks, Mitigation process, security tools**.**

I. INTRODUCTION

Cloud Computing is an on demand service style. At present, it makes everything simple and flexible. But Cloud architecture is complex and is not easy to solve any problem in short. There are three types of clouds is done, such as public, private and hybrid. cloud providers offered three types of Services like Platform as a Service (Peas), Software as a Service (Seas) and Infrastructure as a Service (IaaS) [2].Cloud computing is am most important service system in nowadays. The word "Cloud" is used as a market term [1].

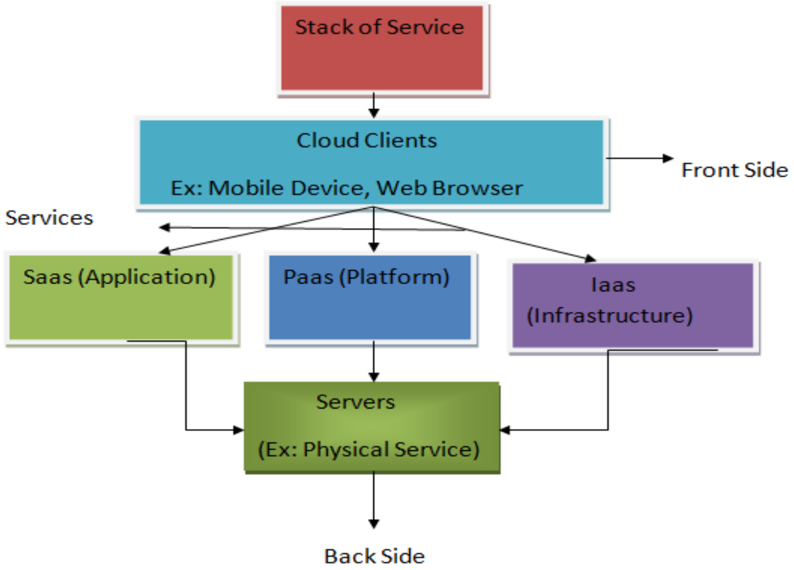

Fig 1: Stack of service (Cloud Computing)

But for some threats cloud computing service is not safe it creates problems between end user and providers. Our main aim is to discuss most of the threats and trying to discuss some overcoming process. In chapter 2 given some related works, after that in Chapter 3 explained some threatened risks & mitigation process, chapter 4 discussed some security tools, finally chapter 5 provides conclusion for the paper

II. RELATED WORKS

In [3] the authors describe the cloud computing security issues. They basically arose the security issues focused on technical security in cloud services. They discuss threatened risks presented in the cloud service like VM-Level attacks, compliance risks, isolation failure, management interface compromise and their mitigation. They also presented cloud security architecture, to protect themselves against threats and attacks. They also find out the key points for this architecture like single-sign on, increased availability, single management console, VM protection, defense in depth approach.

In [4] the author discussed some important threats to ensure a secure cloud environment. This included some security securities (e.g., inside threats, system portability ,access control), software and hardware security (e.g., virtualization technology, data encryption, host operating system, and guest operating system, backup, firewall ,server location etc). The author shows an important issue for the future of cloud security. Vendor lock-in and incompatibility issue also discuss. The author also believes that conventional security concepts can be usefully applied because there are no security standards specific to cloud computing.

In [5] the authors discussed some threats in cloud computing, their characteristics and developing the method. The authors focused on seven most important threats such as Abuse and Nefarious Use of Cloud, Insecure Interfaces and APIs, Malicious Insider, Virtualized Technology, Data Loss or Leakage etc. and some vulnerabilities like Session Riding and Hijacking, Insecure Cryptography, Data Protection and Portability etc. They also discussed that lack of standard may lock-in the clients. Focused on depth security technique & policy should develop to get innovative technology in near future.

III. THREATENED RISKS & MITIGATION PROCESS

Cloud computing is an on-demand service system which provides services as pay –per –use basis' low cost and better service provider. Security is the main fact because the third party is involved here. So some necessary tool and process are discussed to solve that. But there are some threats in cloud computing, and they are explained here.

3.1 Abuse and Nefarious Use of Cloud computing

It is the top threat identified by the Cloud Security Alliance (CSA) [6] . It use botnets to spread malware and spam. IaaS providers provide some opportunity to their customer like unlimited compute, network, and storage capacity. Then attackers take the chance to attack its' vendor.

Mitigation:

Initial registration, credit card monitoring, network traffic monitoring are some process which can reduce this problem.

3.2 Insecure Interfaces

Insecure Interfaces is another threat or cloud computing. The APIs must be secure when it designed, its' authentication, access control, the monitoring mechanism is important.

Mitigation:

Monitoring access control, authentication is allowed strictly it designed.

3.3 Malicious Insiders

In malicious insider, it is very important that which type standard or employee is hired because there is no monitoring or reporting process show their access data.

Mitigation:

Security breach notification system, reporting system through chain management .

3.4 Data Loss & Leakage

Data loss and leakage is a threat which can happen for some reason, such as unreliable media, weak password, no encrypted data, and lack o secure backup system hard drive failure etc.

Mitigation:

Encryption and decryption system, monitoring, file backup, a strong password must apply.

3.5 Account, Service & Traffic Hijacking

Account service and traffic hijacking is another problem that cloud users need to be aware of so that this not happened again. These threats vary from man-in-the-middle attacks, phishing, and spam, to denial-of-service attacks, reused password, fraud, software vulnerabilities .traffic hijacking is a common thread in cloud computing.

Mitigation:

Understand security policy, apply some rules between customer and providers, an authentication process, provide some technique to secure network.

3.6 Denial of Service Attacks

Denial of Service Attacks makes the sense that authorized user are unavailable, sometimes when anyone click on a website, then it show error page or page is not available for Dos.

Mitigation:

An Intrusion Detection System (IDS) can be used to solve this problem [7]. Another detection system is defense federation [8].

3.7 Multi-tenancy natures

This threat attack service provider in online, one provider give service to multiple users according to on-demand service, so the attack can happen normally through VM (virtual machine) this threat affects IaaS. The same application is shared among different users having access to the virtual machine through online

Mitigation:
Strong authentication and access control can identify this threat.

3.8 Risk profiling

It is important for the users or consumers to know software versions, code updates, and intrusion attempt security practices. The user must know where the data or logs are a store. But risk profiling never does that [6].
Mitigation:
Clear information about logs and data, monitoring and alert system can prevent risk profiling .

3.9 SQL injection attacks

Malicious code is inserted into an exact SQL code and it cause a sensitive attack and show some unaccepted result. Unauthorized access to a database sometimes faces this attack.
Mitigation:
Filtering techniques can stop SQL injection, some proxy architecture should develop which dynamically detects and extracts users' inputs for suspected SQL control [9]

3.10 Cross Site Scripting (XSS) attacks

Various types of malicious scripts are added into the web in this kind of attack. It can happen 2 ways like Stored XSS and Reflected XSS.One used permanently; one is not permanently [10.]
Mitigation:
Provide or apply some error-prone data sanitization mechanism, defense mechanism both client -side and server -side.

3.11 Man in the Middle attacks

It is an attracting threat where an entity always tries to stay between a sender and a receiver that means and always give also information between sender and client's they get the wrong information
Mitigation:
To solve this problem a service security, separate endpoint, and server security processes are needed. [11], network topology can change its' configuration.

3.12 Identity theft

It is another threat in cloud computing. Sometimes identity changes one fraud person stolen another person's identity and use all benefits, and or this the victims suffer long run
Mitigation:
Avoid this threat strong password should be used use

IV. SECURITY TOOLS FOR CLOUD COMPUTING

There are some important tools which are used for security. These products promise to protect from malware, help to keep track of who signs into the network, and monitor all others cloud applications such as Salesforce and Google Docs, and more. These are discussed below [12]. Above we already discussed some risk and mitigation tools.

4.1Qualys

It secure devices and web apps & or this no hardware and software are required. If there is any malware found if fix problem, scan apps and safe web apps in cloud security.

4.2 Okta

One of the most important tools, it knows all employee who is accessing information. Identity management is its first work. Main goal o Okta is to provide secure Single Sign-On (SSO) for all the cloud,

4.3. Cipher Cloud

Cipher Cloud is another protecting tool, its' work is to protect all services such as such as Salesforce, Chatter, Box, Office 365, Gmail, Amazon Web Services, and more. It protects that service model through encryption, traffic monitoring, anti-virus scans, and more.

4.4 Bit glass

it provides transparent protection so that reduce loss, aims to reduce the risk of data loss and maintain data's visibility, even within the cloud, it can detect the usage of cloud applications.

4.5 Skyhigh

It can discover, analyzes and secures application which we use in the cloud. It has the capacity to find out or detect which cloud apps the employees are using.

4.6 Antivirus

Anti-virus is an old security tool in cloud computing. Kaspersky lab formula securing virtual machine. McAfee delivers email security.

V. CONCLUSION

In this paper, the basic concepts of threatened risks are discussed & several ways to overcome or handle these threatened risks in cloud computing. Actually, all of this tools and mitigation tools are most important for threatened risk. If these tools are used then almost many security problems can be solved.

REFERENCES

[1] Qi Zhang, Lu Cheng, RaoufBoutaba. Cloud Computing: State-of-the-art and research challenges. J Internet ServAppl (2010).

[2] Rabi Prasad Padhy, ManasRanjanPatra, Suresh Chandra Satyapathy. Cloud Computing: Security Issues and Research Challenges. IJCSITS Vol. 1, No. 2, December 2011.

[3] A. Tripathi and A. Mishra, “Cloud computing security considerations” IEEE Int. conference on signal processing, communication and computing (ICSPCC), 14-16 Sept., Xi'an, Shaanxi, China, 2011

[4] Mathisen, “Security Challenges and Solutions in Cloud Computing” 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST2011) , Daejeon, Korea, 31 May -3 June 2011

[5] Mervat Adib Bamiah* et al. / (IJAEST) INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES AND TECHNOLOGIES Vol No. 26, Issue No. 1, 012 – 015

[6] CSA, “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1” Cloud Security Alliance, 2009, [Online], Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf,

[7] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, “Intrusion detection techniques for Grid and Cloud Computing Environment”, IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, 2010.

[8] Ruiping Lua and Kin Choong Yow, “Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network”, IEEE Network, vol. 25, no. 4, pp. 28-33, July-August, 2011.

[9] A. Liu, Y. Yuan, A Stavrou, “SQLProb: A Proxybased Architecture towards Preventing SQL Injection Attacks”, SAC March 8-12, 2009

[10] P. Vogt, F. Nentwich, N. Jovanovic, E. Kirda, C. Kruegel, and G. Vigna, “Cross-Site Scripting Prevention with Dynamic Data Tainting and Static Analysis”, Proceedings of the Network and Distributed System

[11] Eric Ogren, “Whitelists SaaS modify traditional security, tackle flaws”, Sep. 17, 2009. [Eric Ogren is the founder and principal security analyst at Ogren Group]

[12] http://www.hongkiat.com/blog/cloud-security-tools/