ISSN (Print) : 2229-5429

INTERNATIONAL JOURNAL OF INFORMATION SYSTEMS

(A Journal of SIMCA)

IMPACT FACTOR 5.406

UGC Approved

Vol. VIII, Issue II, January - May 2018

RESEARCH JOURNAL

Index **Pg. No.**

Indexed By:

TOGETHER WE REACH THE GOAL

J-Gate Largest E-Journal Gateway

INDEX

Cloud Computing: A glimpse on Major Security Issues

Sachin G Garde[#1]

[#1]ASM Institute of Management, Shivane, Pune – 411023, India.
sachin.g.garde@gmail.com

Abstract— *"Cloud computing" word becomes famous now a days as the technology have changed everything with respect to various online services available. Different services like Infrastructure, Software, Networking etc. provided by top vendors like Amazon, IBM, Google, and Microsoft Azure. The data which is stored on a remote server can be accessed by the service provider with pay-as-you-go basis. The data stored on remote server is really secured or not is still an issue. In this paper, I would like to emphasize on major security issues in cloud computing.*

Keywords — Cloud Computing, pay-as-you-go, APT, DDos, Major Security issues.

I. Introduction

Cloud computing is nothing but inter networking (internet) based computing services which is provided through internet to the different users across globe. Data has been collected (with the help of various online web applications/portals) and must be stored on some server which is actually at the remote location or may be at the local site (depending on the storage vendors and their physical data centres). The services provider provides various services on pay-as-you-go basis to store and fetch back this data as and when required to the customers; this means paying for a service before it is (any service) used with SLA (Service Level Agreement). This SLA has been made between service provider and consumer with consent amongst the involved parties to agree upon.

The following services has been provided by these top vendors like PaaS (Platform as a Service), IaaS(Infrastructure as a Service), SaaS(Software as a Service) etc.

PaaS – Under these services, everything has been provided to the consumer from the start like OS, Design, Development, Web Services like hosting an application with integration, server security options etc. In this, consumer should not be worried about the platform on which a particular product has been designed and developed and the related concerns. This should be taken care by vendor itself.

e.g. Microsoft Azure, Rackspace Cloud sites, VMforce, Google App Engine etc.

IaaS – Under these services, infrastructure resources has been provided like hardware, network, data resource etc. In this, consumer has to only pay for the infrastructure utilized by him/them, the rest will be taken care of vendor.

e.g. Amazon EC2, Rackspace Cloud servers, Atlnda RTI

SaaS – Under these services, consumer need not be worried about designing and developing of software and their storage and fetching back the stored records as and when required, but the vendor will take care of those things as he has provided the service for this and a consumer has to pay for this service.

e.g. On-demand CRM provided by salesforce.com, On-demand email (e.g. hosted Exchange, Google mail) etc., Web conferencing (e.g. WebEx, Citrix on-demand)

II. Types of Cloud

There are three different ways cloud

a. Public cloud – These clouds are owned and operated by a third-party vendor again on pay-as-you-go basis, which delivers their computing resources like servers, storage over the internet. e.g. Microsoft Azure. Using a simple web browser you can be able access these services and manage account. With the help of public cloud, Software, Hardware and other infrastructure has been managed by vendor itself.

b. Private cloud – As its name suggests, its a private one and is owned by a single person, business entity or an organization. Some companies opt a third party service provider to host their web site or on a private cloud. A private cloud can be also physically located on the company's on-site data center as well.

c. Hybrid cloud – In this type of cloud, all above types should combine together by technology which allows data and applications to be shared between them. Hybrid cloud provides business flexibilities and more deployment options by allowing data and applications to move amongst public cloud and private cloud.

III. Essential Characteristics of Cloud Computing

a. On-demand Self Service – A consumer, by himself can have computing capabilities like server time and network storage as needed automatically without requiring human interaction with each service provider.

b. Extended access – With the help of odd thick or thin client platforms, we can easily access our electronic gadgets like mobile phones, laptops, tablets, workstations etc. through standard mechanisms.

c. Resource pooling – Various resources like storage, memory, processing have been pooled at the remote server (it could be locally managed or within the country or a specific data center at remote location) to save and retrieve back to the consumer as and when required. Generally consumer need not to know the

actual location, where is the storage of their data actually resides.

d. Fast flexibility – Services provided by cloud computing are fast and flexible as per consumers need.

e. Measured service – Well controlled and optimized resources has been initiated by service provider[1] like how much storage capacity can a consumer can choose, how much processing speed of their transactions can they afford, also how much bandwidth they can choose for processing of these transactions, how many active user accounts they can afford. etc. These resource usages can be observed, controlled and recorded as per SLA.

Major Security concern in cloud computing – A very recent study says that "APT's and DDoS attacks are considered more serious than viruses and botnets"[2].

IV. CLOUD DEVELOPMENT TOOLS

Following some of the tools has been used for development purpose for cloud computing, which enables a developer directly develop their applications without downloading it on to their individual machines [3].

a. **Otixo** – It is a web based tool for cloud user. It is like a file manager for all our cloud services and social networking sites. This tool supports for Amazon S3, Google Drive, SkyDrive, CX, DropBox, Face book etc. we can achieve all cloud services with single permission.

b. **Hojoki** – It's an IOS and android based tool used to provide collaboration of different cloud services. e.g. Evernote, Google Drive, Drop Box, Sky Drive etc. It can be used for collaborated services, tasks management and also forget notification from connected application.

c. **CloudFuse** – It is desktop based application which allows only one sign in for different cloud based services. With the help of this one can manage data on the cloud across different clouds like Drop Box, Google Drive, Sugar Sync etc. Using this one can be able to create, update, remove and rename folders, dragging and dropping items between desktop, also share the information amongst other machines.

d. **Aneka** – This tool is one of the flexible, extensible cloud application development tool, which allows servers and desktop machines to be linked together to form a very powerful computing infrastructure. It provides flexible and configurable execution platform, its Application Programming Interface supports very famous cloud programming models namely, i) Task, ii) Thread and iii) Map Reduce.

Ubuntu server introduces a technical preview of Juju, a modern approach to service deployment and orchestration on cloud which supports Ap architecture.

e. **Nimbus** – It is an open source and compatible w IaaS. It provides the features to scientific commun such as updating in proxy credentials, batch schedul The Amazon Elastic Compute Cloud (EC2) considerably the best one, but Manjrasoft Aneka 2.(market oriented which supports cloud development management with rapid application developm (RAD) and having its own distribution capabilities.

V. MAJOR SECURITY CONCERNS

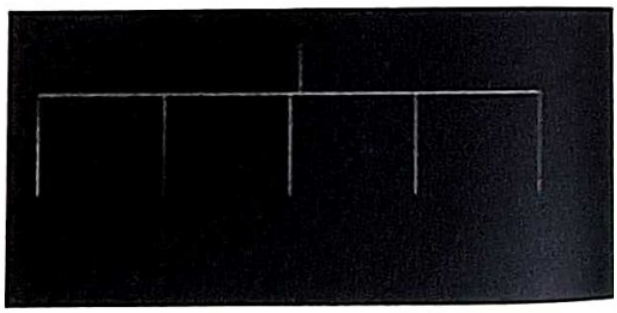
A. *APT* – (*Advanced Persistent Threats*) – As per definiti it refers to a group, such as a foreign government, w both the capability and the intent to persistently effectively target a specific entity.

a. The most targets of APT's are smaller organizatio also law firms have been attacked to target patent by foreign interests (starts with 'C' and end w 'hina'[3] so that intellectual property could eliminated. While patents are being authored (i.e. p to filing).

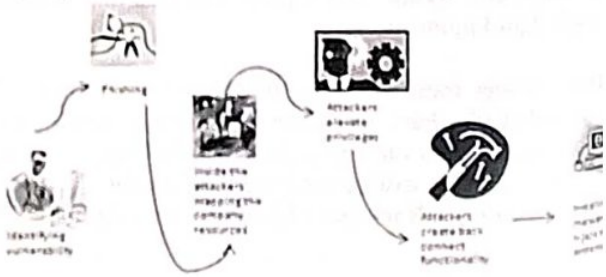
b. APT's can be able to hack down the top secret acquire trade secret, classified information etc.

c. Traditional security systems such as anti-vi malware removal software and perimeter secu systems are found to be useless during these attac Most of the organizations have accepted the fact once the breach has been done, only then secu concerns are come into the picture.

These threats can be divided into 5 stages as follows:



To identify, who is inside the cloud is very hard to de How they can do this is depicted graphically as below [3]



The process involves

1. To Identify vulnerability
2. Phishing
3. Inside the attackers mapping the company resources
4. Attackers elevate privileges
5. Attackers create back connect functionality
6. Installing malware to hijack the systems

DDoS – (Distributed Denial of Service) – In this, attackers are a group of machines targeting a particular service [4]. The increasing number of reports of DDoS makes most fatal threat amongst other known threats. A recent study shows that more than 20% of enterprises in the world experiences at least one DDoS attack incident on their infrastructure [5]. Some of the following examples show that DDoS threats are more vulnerable than any others.

a. Lizard Squad attacked cloud based gaming services of Microsoft and Sony which took down the services on Christmas day in 2015.

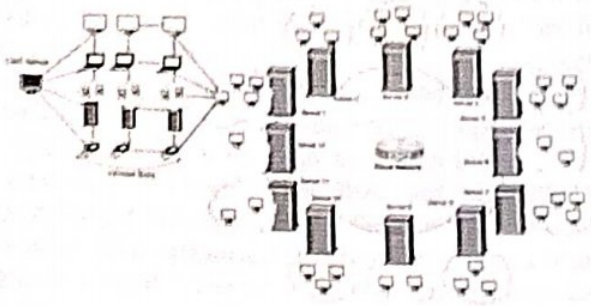
b. Cloud service provider, Rackspace, was also targeted by massive DDoS attack on its services.

c. Another example of DDoS attack faced by Amazon EC due to which a heavy down time had experienced. Also because of down time, the organization suffered business loss and man long term and short term effects on their business expansion.

d. A report by Verisign iDefence Security Intelligence Services [6] shows that SaaS cloud service sector has been hampered a lot during last year.

e. With respect to Virtual Machine's (VM), the "elasticity" or "auto-scaling" faced economic losses based on DDoS attack which is also known as Economic Denial of Sustainability (EDoS) attack or Fraudulent Resource Consumption (FRC) attack [7].

f. IaaS has also been hampered as the machines have been utilized with the help of Virtual Machine (VM's) on-demand by the cloud consumer (e.g. commercial web applications or web portals). Following figure focused on utilization of VM's on server for cloud computing environment.



Malware Injection – The coding for the malware is just like normal program script, embedded into cloud services which will eventually act as a valid instance and run as a SaaS to cloud servers. Indirectly the infections (malicious code) have been spread into cloud services as a part of the software or service that is running within the cloud servers themselves.

Once this script (malicious code) has been executed and the cloud begins operating it repeatedly, attackers can be able to have the sensible information and they can steal the data.

A very recent study says that because of malicious code an APT attack against financial institutions around the world may be considered as one of the largest cyber heist till date. Unlike the usual cybercriminal method of stealing consumer credentials or compromising individual online banking sessions with malware, the brazen Carbanak gang targeted banks internal systems and operations, which results in a multichannel robbery that averaged $8 million per bank [8]. Also to target a LAN (Local Area Network), a LOWBALL malware have used for spear phishing campaign in December 2015 a FireEye report revealed this report [8].

Very recent example has been found in Brazil, where, CloudSquirrel infects users by downloading malicious encrypted payloads via a JAR (Java ARchieve) file. Payloads contain information and password stealers. Once the cloud malware establishes a connection with its Command & Control hosted in Dropbox, its commands acts like as a plain text files with fake extensions such as .png, .wmv,.dat, .mp4 etc [8].

D. **Insecure API** – (Application Programming Interface) This gives user an opportunity to customize the applications on cloud.

As API's are user friendly, they can become a threat to t cloud security. API's having customizable features whi will allow customers to enhance their business needs per their requirement as and when required. Due to wh there should be an exploitable security risks involved cloud services.

E. **Abuse of Cloud Services** – As in this digitization wo every organization has come up with some cloud b services because of their features provided by the ven along with SLA including massive data sto management.

This feature of massive data storage capacity may hackers and unauthorized users to easily host and s malware, illegal software and other digital prop Because of this, entire business can be hampered. D which the terms of use can be renegotiated.

These risks include sharing of pirated software, v music or books and can result in legal conseq depending upon the nature of infringement.

VI. CONCLUSION

The security issues considered in this paper are information and awareness, apart from this, there ar such concerns in cloud computing but those w

considered as harmful as APT and DDoS. Thats why major focus was concentrated on those two concerns.

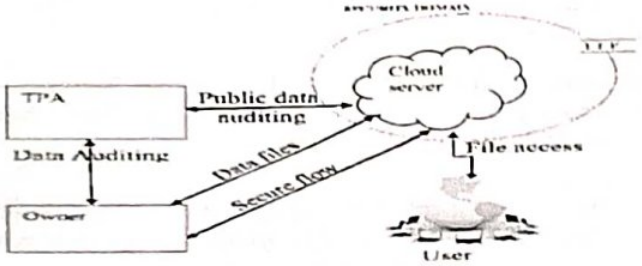
Also the optimal solution for the security concern requires depth of technical knowledge and expertise, also having the ability to pursue it thoroughly. As far as data security is concerned, the hash file approach and meta-data approach [9] could have the best solution.

As far as APT is concerned, the conceptual approach to ensure security to cloud [10] and Algorithmic approach for securing cloud [10].

In conceptual approach, TTP (Trusted Third Party) and TPA (Third Party Auditor) plays a vital role where TTP ensures secure interaction between two parties and TPA ensures strong authentication and authorization between them.

In this, cryptography is used to ensure secure transmission of data files over a network. Security auditing is also another way to verify the presence and functioning of the cloud customers and cloud providers as security mechanisms. TPA can also perform MAT (Multiple Auditing Tasks) for single or multiple clouds in branch manner for better efficiency and security [10].

Following diagram shows the secured model of cloud.



In an Algorithmic approach, divide the data into different n parts by secure scanning of data process, say S and different parts, say D1, D2, D3, ..., Dn. When the data is to be shared between multiple clouds in secured way, the cloud is given an access to the data shares securely [10].

As far as DDoS is concerned, the application level defense, VM/OS level defense, Hypervisor level defense, Cloud level defense, ISP level defense [7],under ISP level defense, major solution designs could be proposed like Application defense, Application defense and System defense and System defense or System defense and External defense and also combining all the three i.e. Application defense and System defense and External defense. All those elaborate the best way to secure cloud computing in effective manner with different perspectives.

As far as malware injection attacks are concerned, databases should not exposed to the internet. They should be accessed only through local host during setting up these kinds of web applications.

Also utilizing proper authentications and authorizations to the different database users and access control mechanisms should be adopted before internet connectivity. The incoming requests can also be checked that the requests are legitimate or not, if those are not, avoid such requests and prevent such requests in future by various encryption algorithms.

As far as Insecure API's are concerned, user roles and their related permissions should be appropriately mapped during development of application, so that further breaches could be avoided. Also in case of dynamic applications, user rights should be granted automatically and revoked again, once their work is over.

VII. ACKNOWLEDGEMENT

I would like to thank you the anonymous reviewers for their valuable suggestions and references.

REFERENCES

[1] National Institute of Standards and Technology, U.S. Department Commerce, Peter Mell, Timothy Grance

[2] Security Report - The Evolving Role of CISOs and their Importance the business, August 2017, Ponemon Institute

[3] Chandini Sasanapuri, Sudhakar Ch, Chilsi Hasan K.C, Narasimh Challa "Classification of APT's and Methodological Approach Secure Cloud Services" International Journal of Applied Enginee Research ISSN 0973-4562 Volume 11, Number 2 (2016) pp 1000-1

[4] J. Mirkovic, P. Reiher, A taxonomy of DDoS attack and DDoS def mechanisms, SIGCOMM Comput. Commun. Rev. 34 (2) (2004) 53, doi:10.1145/ 997150.997156

[5] P. Nelson, Cybercriminals moving into cloud big time, report 2015, (http://www.networkworld.com/article/2900125/mal cybercrime/ criminals- /moving- into- cloud- big- time- report.html).

[6] Tara Seals, Q1 2015 DDoS attacks spike, targeting cloud, 20 http://www. infosecurity-magazine.com/news/q1-2015-ddos-at spike/).

[7] Computer Communications (107) (2017) 30–48 "DDoS attack in Computing: Issues, Taxonomy, and future directions", Gaurav Sa Manoj Singh Gaur, Dheeraj Sanghi, Mauro Conti, Rajkumar Buy

[8] THE TREACHEROUS 12, Top threats to cloud computing - In Insights, https://cloudsecurityalliance.org/group/top-threats/

[9] Providing Confidentiality and Integrity on Data Stored in Storage by Hash and Meta-data Approach, International Jou Advance Research in Engineering, Science & Technology e 2393-9877, p-ISSN: 2394-2444, Vol. 4, Issue 5, May 2017, Jee Prof. Prashant Modi

[10] Classification of APT's and Methodological approach to secur services, International Journal of Applied Engineering Researc 0973-4562 Vol. 11, Number 2 (2016) pp 1000-1005, C Sasanapuri, Sudhakar Ch, Chilsi Hasan K.C., Narasimham Cha