*THINK INDIA JOURNAL*

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

# Taxonomy of Security Issues and Attacks In Cloud Co Mputing

**SIMRANPREET KAUR**

**SCHOOL OF COMPUTER SCIENCE AND ENGINEERING**

**LOVELY PROFESSIONAL UNIVERSITY, PHAGWARA, PUNJAB, INDIA**

**Abstract-**. Cloud computing is undoubtedly a promising technology. It offers on-demand services to its users. With this, users do not have to be concerned about infrastructure expenditure and personnel training. However, it is fraught with various security issuesthat create hindrance in its global acceptance by organizations. Companies are reluctant to store their critical business related data on the cloud. Certainly, it is important to work on security aspect of this technology. This paper's prime focus is on overview of cloud security, security threats, attacks that has paralyzed it.

**Keywords**- cloud computing, threat, attack,vulnerable, security.

## I. INTRODUCTION

In today's world where technologies like, grid computing, cloud computing etc. are being used enthusiastically owing to their advantages, itis imperative to put focus on security issues pertaining to them. Major security issues causing hindrance in adoption of cloud are: threat to data confidentiality as well as. Second factor of concern is the ownership of resources by provider, and this is owing to the fact that the host systems are not worthy of trust every time. It is indeed difficult to ensure security as well privacy of data in an environment where resources are distributed and shared [1].Ensuring that data is accessed only in accordance with planned terms demands well organized security measures. Finally, the third factor is the shortfall of standard methodology for designingService Level Agreement [2].

In this paper, Section II focusses primarily on threats in cloud computing. Section III entails security attacks in cloud and their solutions. Section IV finally, concludes the paper.

## II. SECURITY THREATS IN CLOUD COMPUTING

*A.* As per Cloud Security Alliance (CSA), various security threats in cloud environment are of following types as shown in figure 1 [3][4].

1. Malicious insider

Confidential data is vulnerable if the attacker is an insider. Organizations generally do not specify their recruitment process and how their employees are accessing the resources. Clearly, some malicious intended employee could misuse the privilege and gains control over cloud services and critical data. Activities of insiders go unnoticed by intrusion detection systems as they are considered as legitimate ones. It is imperative to have more transparency in not only security but also management process, if this concern has to be dealt with.


Copyright © 2019Author

ISSN: 0971-1260
Vol-22-Issue-3-July-2019


Figure 1: Security threats in cloud computing

2. Shared technology issues

In IaaS, infrastructure is shared. Time and again, underlying components are not designed in a manner to impart strong isolation to support multi-tenancy. Thus, hypervisor is used to fill this gap. But hypervisors are not flawless due to which one tenant cause hindrance in working of other, thus, affecting the overall working of the system. For remedial purposes, security practices for configuration could be implemented, strong authentication could be put to use.

3. Abuse of cloud computing

In cloud environment, users are servednumerous utilities including network, storage etc. Some providers offer free trial period. Attackers misuse this free trial and pose serious concerns because attackers plant malicious codes and get away without being detected. Recent concerns include key cracking, DDoS attack. For remedy, stringent registration and validation process, proper monitoring of network traffic could be used.


Copyright © 2019Author

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

4. Insecure interface

Interfaces or APIs are used by customers to interact with cloud services. Functions performed by the interface are: management, monitoring, provisioning etc. Apparently, ensuring the security of APIs is of paramount importance so as to have unhindered services from cloud. Vulnerability in these interfaces leads to serious issues like improper authorizations, anonymous access due to inefficient access control, reusable tokens. As a remedy, encrypted transmission apart from strong authentication could be used. At the same time, pertinent security model for interface is essential.

5. Data loss

Shared and dynamic nature of cloud has given birth to major issues that includes data being compromised, deleted, and updated without keeping copy of original data. In worst cases, data becomes unrecoverable. Insufficient authentication, inconsistent and inefficient encryption techniques are some instances of threats in this category. As a remedy, strong key generation algorithms must be used, retention policies should be clear, efficient API security be used.

6. Service hijacking

In cloud computing, phishing attack, re-usage of passwords or other credentials, fraud pose serious threat. Once, attacker accomplishes his access to user's credentials, then it becomes easy to eavesdrop on activities, return incorrect information or even redirect user to illegitimate sites. Making user's account or service instance as a platform, attacker can launch new attacks. As a remedy, there should not be any sharing of credentials between users and services, efficient two-factor authentication must be used, intense monitoring to find unauthorized activity.

7. Unknown risk profile

Cloud computing allows organizations to focus primarily on business rather than being worried about hardware and software requirements. However, this makes them unfamiliar of security procedures, logging process used. Knowing who is sharing information along with you is also important. So, it leads to unknown exposure to security threats. As a remedy, vendor must disclose log information, data information. Infrastructure details etc.

*B.* As per Gartner[5], there are certain concerns like :

- Privileged user access
- Regulatory compliance
- Data location
- Data segregation
- Recovery
- Investigative support
- Long term viability.

All these are explained in figure 2. These must be considered before choosing a cloud vendor. In cloud computing. Customers must ask for transparency from vendor in order to have secure environment.


Copyright © 2019Author

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

## Privileged user access

- Outsourced services are less secure than in-house services. There is a certain level of risk posed on data processed outside the enterprise. So, according to gartner, it is imperative ti know about people maanging your data.

## Regulatory Compliance

- Cloud computing vendors who refuse to undergo audits and scrutiny are hinting that customers are themsleves responsible for their critical data's integrity and security.

## Data Location

- In cloud environment, location of data in unknown. Customer must inquire from vendor about local privacy requirements and whether proper rules for processing data are followed or not.

## Data Segregation

- In cloud, data from different customers are in a shared environment. Even though, encyrption is used but it shuld be verified that provders are using efficient techniques fro encryption and are fully tested. Any failure with encryption could result in data being unavailable.

## Recovery

- Customer is unawasre about the location of data in cloud. Even then, vendor should furnish information whether data will be fully recovered and in what time, in situation of a disaster.

## Investigative support

- Data hosts in cloud environement keeps changing which makes investigation of data a tedious task. In case the vendor doesnot provide a contract to support investigation then it has to be assumed that investigation requests are impossible

## Long term viability

- Even though, cloud companies usually donot get broke or taken over by a lerger company, yet ensuring availabilty of data is imperative. Customers must ask how would they get their data abck if such scanrio ever arises.

Figure 2: Security concerns in cloud computing [5].


Copyright © 2019Author

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

## III. SECURITY ATTACKS IN CLOUD

Due to vulnerabilities in cloud, attacker is able to fulfil his objective of first detecting the vulnerabilities and then exploiting them. Following are few attacks launched by and attacker.

### 1. Metadata spoofing attack

This attack is caused due to tampering of metadata document, commonly, known as Web Service Definition Language (WSDL). Information pertaining to we service allocation are gathered in this document. Once, attacker wins in making alterations in WSDL then intense consequences are found. For an instance, *deleteUser*could be modified to *setAdminRights*. With this, the users who were supposed to be deleted would now become authorized users with administrative privileges. For security purposes, strong encryption techniques along with secure authorization could be used [6]

### 2. Zombie attack

This attacks falls in the category of DDoS (Dedicated Denial of Service) attack. Here, attacker, known as zombie, paralyses the availability of services by victim by sending multiple requests to overload it. It may happen that the parties in the attack are all in cloud. As a consequence of huge requests, cloud provider heightens up the computational power, thus, leading to exhaustion of server's resources and making it unable to serve other instances. For security, efficient authentication and authorization could be used [7].

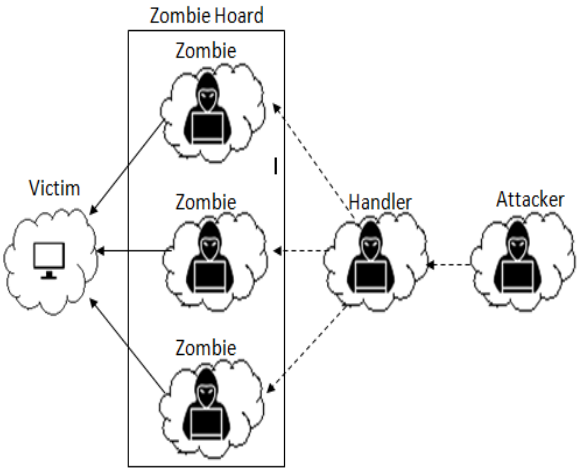


Figure 3: Zombie attack[8]

### 3. Phishing attack

In this type of attack, a web link is used to redirect the user to false link with the intention of accessing user's private credentials. Attacker might use cloud for hosting phishing attack site and could also hijack accounts of other users in the cloud. For security, strict monitoring and proper identification of spam mails is necessary [9][10].


Copyright © 2019Author

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

### 4. Service Injection attack

Attacker injects malicious service or a new VM into cloud system. Cloud functionalities are changed by malware. Attacker might create his services like SaaS, PaaS, or IaaS and makes it a part of Cloud system. Due to this, valid user requests are redirected to malicious services. For security, service integrity checking must be used, isolation between VMs could also help[11].

### 5. Backdoor channel attack

In this, attacker might conquer remote access to a compromised system. Backdoor channels could be used to handle victim's resources and turning them into zombies. These zombies are then further used to launch DDoS attack. For security, isolations between VMs and proper authentication could be used[11][4].

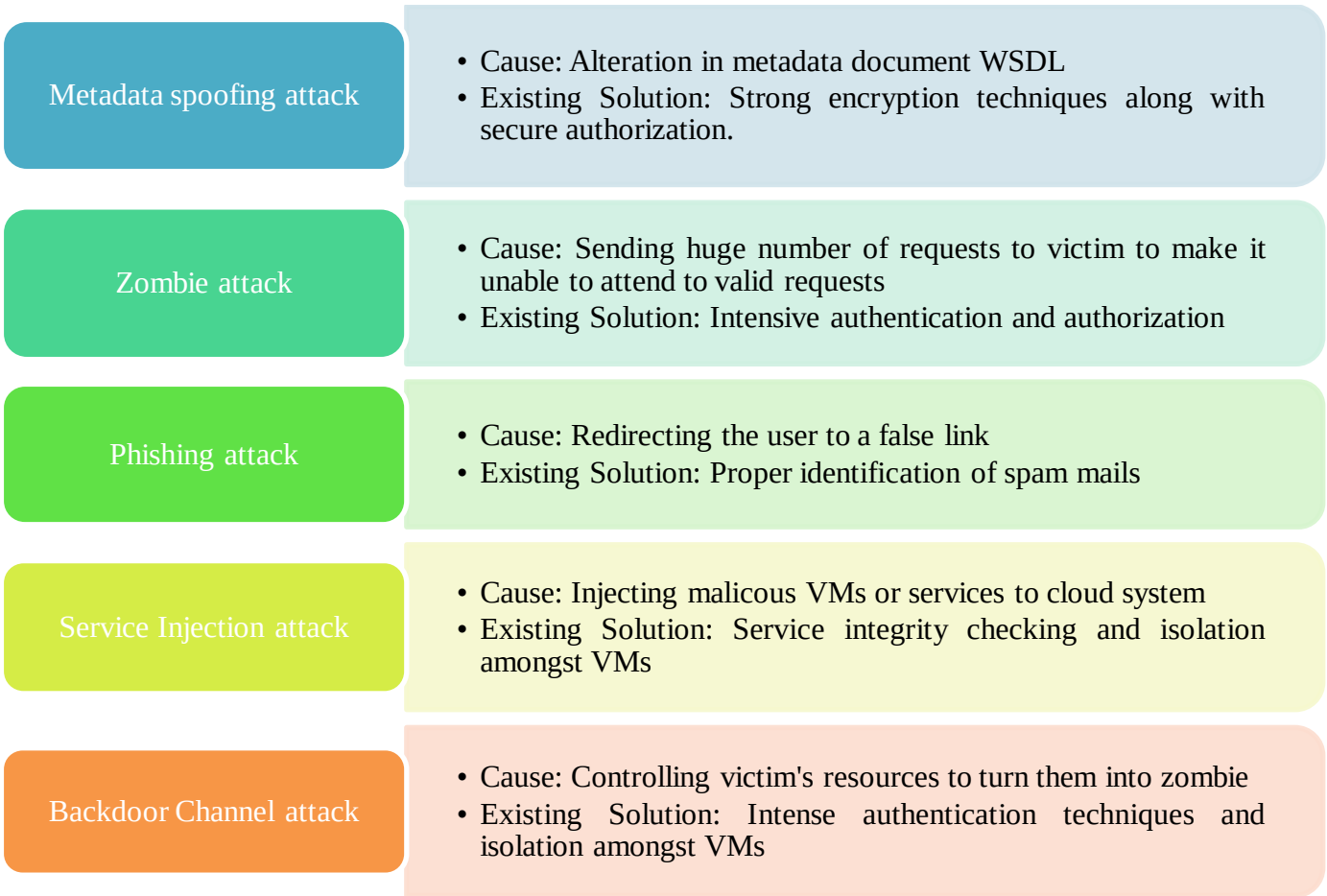


Figure4: Summary of security attacks in cloud computing


Copyright © 2019Author

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

## IV CONCLUSION

It has become important that organizations are aware of security threats in cloud computing. This paper has highlighted various security concerns and attacks in cloud that has caused hindrance in its adoption. Also, existing solutions for various attacks are also enlisted. In the future, the vulnerabilities in cloud platform has to be dealt with and stronger techniques for authentication, authorization, and encryption are required so that benefits of cloud could be realized to its full potential.

## REFERENCES

[1] Security threats. Microsoft. http://technet.microsoft.com/en us/library/cc723507.aspx

[2] KR. Balachandra, VP. Ramakrishna, A. Rakshit, "Cloud security issues", In: Proceedings of the 2009 IEEE international conference on services computing, SCC'09, pp 517–520, 2009.

[3] "Threats and Opportunities with Cloud Computing", Cloud Computing Strategies, 109–131. doi: 10.1201/9781439834541-c5, 2010.

[4] M. Durairaj, and A.Manimaran, "A study on security issues in cloud based e-learning", Indian Journal of Science and Technology, 8(8), pp. 757-765, 2015.

[5] J. Heiser J, What you need to know about cloud computing security and compliance, Gartner, Research, ID Number: G00168345, 2009.

[6] B. Grobauer, T.Walloschek, and E. Stocker, "Understanding Cloud Computing Vulnerabilities", IEEE Security& Privacy, 9(2),pp. 50–57, 2011.

[7] P.Revathi, "Flow and rank correlation based detection against Distributed Reflection Denial of Service attack", In 2014 International Conference on Recent Trends in Information Technology , IEEE., pp. 1-6, 2014.

[8] M. Jouini, and L.B.A Rabai, "A security framework for secure cloud computing environments", In Cloud security: Concepts, methodologies, tools, and applications, pp. 249-263, IGI Global, 2019.

[9] B. Krebs, Salesforce.com Acknowledges Data Loss, Security Fix, The Washington Post, 2007.

[10] R. McMillan, Salesforce.com Warns Customers of Phishing Scam, PC Magazine, IDG NewsNetwork,,http://www.pcworld.com/businesscenter/article/139353/salesforcecom_warns_customers_of_phishing_scam.html, 2007.

[11] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, " A survey on security issues and solutions at different layers of Cloud computing", The journal of supercomputing, 63(2), pp. 561-592, 2013.


Copyright © 2019Author

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

[12] U. Kumar, and B.N. Gohil,"A survey on intrusion detection systems for cloud computing environment", International Journal of Computer Applications, 109(1), 2015.

[13] S. Kaur, R. Kaur, R., and A.K. Verma, A. K," Jellyfish attack in MANETs: A review", In *2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, pp. 1-5, IEEE, 2015.


Copyright © 2019Author