ISSN 2319 - 5975

Volume 7, No.6, October - November 2018

International Journal of Networks and Systems

Available Online at http://www.warse.org/IJNS/static/pdf/file/ijns01762018.pdf

https://doi.org/10.30534/ijns/2018/01762018

Review on security challenge faced organization based on-cloud computing

Aisha. O. Albadrany [1], **Mohammed.Y. Saif** [2]
[1] Taibah University, Saudi Arabia, Aishaalbadray@taibahu.edu.sa
[2] Taibah University, Saudi Arabia, Mohdya12@taibahu.edu.sa

ABSTRACT

With the advancement of technology. Cloud computing has emerged which has revolutionized in the technical world. today a lot of business and organizations has developed its operations by using cloud computing techniques .it provides many major services to organizations and enterprise and represent as a key role in increasing the efficiency of its work.

Although all these advantages of cloud computing, the security aspect of information and the protection of resources are the biggest concern of these institutions so the organization management focuses on getting the high guarantee for protecting data.[3][9]

In this paper, we review all security challenge faced organization and enterprise based-on cloud computing and how these challenges affect the security elements. also, we discussed different types of security challenges. and we have classified them to threats, vulnerabilities, and attacks. with its definition, the method used and The protecting strategies used for each category were also clarified. Then we explained some defensive procedures to ensure that the cloud computing technique has strong security architecture and what mechanisms management needed to reach the highest levels of security for the different organizations.

Key words : About four key words or phrases in alphabetical order, separated by commas.

1. INTRODUCTION

In last years, cloud computing technology has introduced many services to organization. like storage, access, manipulate, retrieve or work data from anywhere by connecting with cloud server using internet. all this processes are managed by cloud services provider. cloud computing services increase the efficient of organization works. so no need to use a lot of physical hardware or more employee. also by cloud computing services we reduce the potential of loss data. but information security aspect is the major concern for every organization nowadays. if cloud services provider doesn't protect the data, then their loss them customers as his data not at safety side . Protecting critical files and data is very important. The organization will may loss data and resources. if there were not strong security procedures. while many malicious software is emerging daily. also using and development a new hacking tools not exclusive on professional person .[1][7].

1.1 Research questions:

A. What is the security challenges faced organization which using cloud computing services?

B. What is the methods and protecting strategies for each challenge?

1.2 *General Security Challenges:*

Data in organizations that based on cloud techniques are exposed to many security challenges. Some are within the organization itself and some are when transferred from the organization to servers. Even after storing them in servers, they are subject to a set of risks like (Denial of service , Malicious code, Unauthorized access ,Inappropriate usage ,Multiple component).[1][3][10]

In Table (1) we explained set of this challenges.

Table 1: Security challenges on cloud computing architecture

Stage name	Security challenge position	Attacks type	Security affected element
Cloud computing provider.	1-Data base center. (software) 2-Storege devices and servers. (hardware) 3-protected software. 4- Employees.	1-data loss. 2-data breaches. 3-natural disaster. 4-danial of service 5-disable protected software. 6-insider malicious.	• Integrity. • Confidentiality. • Availability.
Data transmission.	1-data and files. 2-transfere media.	1-unauthorized access. 2-maliciouse code. 3-Inappropriate usage.	• Integrity. • Confidentiality.
Cloud computing customer(organization)	1-local data center. 2-data and files. 3-legal contract. 4-Employee.	1-outsider malicious. 2-insider malicious. 3-Inappropriate usage. 4-malicious code.	• Integrity. • Confidentiality. • Availability.

2.SECURITY CHALLENGE CLASSIFICATION

To ensure high security level in organization based on cloud computing, first must discover all security challenge related to all asset side. define security challenges exactly is very important thing, to know where a weakness points, then try to find best solution. [7][9][10]

we can divide security challenges to: threats, vulnerabilities and attack as following:

a) Security threats

Any properties that exploit a vulnerabilities or weakness points to cause harm computer asset. Threat may or may not happened but has potential to damage data and but all resources at risk. for example, the attacker can use fishing and backdoor to gain some information then used in enter to network and loss data. [2] [5]

threat example includes:

1. *Data Breaches.*
2. *Data Loss.*
3. *Account Hijacking.*
4. *Abuse of Cloud Services.*

b) Security vulnerabilities

Vulnerability is exploiting a weakness by attackers to perform unauthorized action. threats take vulnerabilities to risk place. Information security must discover all vulnerabilities points to ensure the security in a high level. Here list of vulnerabilities examples:

1. *Vulnerable Systems and APIs .*
2. *Shared Technology Vulnerabilities.*
3. *Lacking Due Diligence.*
4. *Weak Authentication and Identity Management.*
5. *Insufficient Security Tools.*
6. *A Lack of Responsibility.*
7. *Human Error.*
8. *Unprotected IoT Devices.*

c) Security attack

Computer attacks include any attempt to access computer resource and data, through unauthorized way. attacker may just monitor traffic network or he steal critical information or disable access to files and asset. There are many types of attacks like, Denial of Service attack, malicious insider, fishing and Advanced Persistent attack. Ransomware and Spectre and Meltdown are new types of attacks.[1][2][4] In the table (2) below list the security threat types with more details.

Table 2 : Security challenge detailed and its defense strategy

No.	Security challenge name	Security challenge definition	Security challenge methods	defence strategy
1	Data Breaches	access to data by unauthorized party. Then copy, move or edit this data.	Targeted Attack.	1-apply strong security techniques. 2-perform best security practices.
			Simple Human Errors.	
			Application Vulnerabilities	
			Poor Security Policies	
2	Data Loss	unavailability of data or incorrectly data form as result of natural disasters.	Natural Disasters	copy all files and data in many location .
			Simple Human Errors	
			Hard Drive Failures	
			Power Failures	
			Malware Infection	
3	Malicious Insiders	include all threats from insider party that can acquire and editing data like system administrator, inside employee and contactors.	Former Employee.	1-Perform pest training on security side. 2-Apply strong security policies .

			System Administrator Third Party Contractor Business Partner	
4	Denial of Service (DoS)	Using on Machin to send many of untruth request to server which caused due prevent original request from access to server	Weak Network Architecture Insecure Network Protocol Vulnerable Application	Detection software against of(DOS)
5	Vulnerable Systems and APIs	any weakness in system or application interfaces can attackers exploit them to corrupt data .	Weak API Credentials Key Management	1-Design protected (API). 2-copy all files and data in many location.
6	Weak Authentication and Identity Management	weakness in process that aims to proving the identity when accessing data or application	Social Engineering Attacks Man-In-The-Middle (MITM) Attack Malware Infection	Customize suitable permission for each user.
7	Account Hijacking	identity theft by hackers to use account to steal data or to deploy malicious software.	Social Engineering Attacks Man-In-The-Middle (MITM) Attack Malware Infection	1-mitigate the sharing of account credentials. 2-enable multifactor authentication
8	Shared Technology Vulnerabilities.	exploit weakness in shard technologies.	VM Vulnerabilities Hypervisor Vulnerabilities Third-Party S/W Vulnerabilities	1-apply strong isolation techniques. 2-perform best security practices.
9	Lacking Due Diligence.	neglect cloud service provider in due diligence.	No Auditing Service Level Agreement	1-review (CSP) standards continuously.
10	Advanced Persistent Threats (APT) .	access to network for monitors network operations and steal information.	Spear Phishing or Wailing Direct Hacking USB Malware Network Penetration Third-Party APIs	1-Advanced security controls. 2-monitoring infrastructure. 3-hard process management.
11	Abuse of Cloud Services .	abuse using cloud resource for any illegal process.	No Cloud Service Monitoring Service Level Agreement	training on best using of cloud services.
12	A Lack of Responsibility	A lack of responsibility by employees.	Human Negligence Service Level Agreement	Increase security awareness
13	Insufficient Security Tools	Use weakness security tools to harm data	Insufficient Security Tools	Improve security tools
14	Human Error	All errors resulted as human.	Human Negligence No or Insufficient Security Training	Increase security awareness.
15	Ransomware	a malicious software used encryption to locks all data and files.	Infrastructure Vulnerabilities Platform Vulnerabilities Application Vulnerabilities	1-ensure the integrity of infrastructure. 2-using protected software.
16	Specter and Meltdown	a set of vulnerabilities effect to computer chips.	Hardware Design	Advanced security controls.

3. CLOUD SECURITY MANAGEMENT

To ensure that cloud computing architecture has effective against threats and attacks .it must perform strong defensive methods as a key in security management. security control has set collection of procedure to protect and treat any vulnerabilities.

3.1 Deterrent controls procedure

These procedure aims to reduce attacks on data. by using a warning sign on private resources and report the attackers that maybe have exposing adverse consequences in a state perform attacks**.**

3.2 Preventive controls procedure

Preventive controls procedures are intended to strengthen the system against attacks. by eliminating weakness or reducing. also by using Strong authentication for each user. therefore, will unauthorized users not be able to access data.

3.3 Detective controls

The aims of Detective controls procedure are to detect and resolve any incidents. In the event of an incident, a detective control will signal the preventative or corrective controls to react the attack. by using security monitoring of network, like intrusion detection and prevention arrangements supporting communications infrastructure.

3.4 Corrective controls procedure

Corrective controls procedures are intended to reduce the risk of an incident, usually by limiting the damage, and by Restoring system backups to rebuild a system is the most example of a corrective control procedure.[7]

4.THE PRACTICAL IMPLICATIONS

The practical implications of this research results are development of a new security model to increase the security side. and reducing losses resulting from any security threats. also this result help to increase protecting methods used into files and data, and increase security a awareness for employees The results of this study can be used by stakeholder individuals who are in charge of securing the assets of their organizations and institutions and want to improve protecting the confidentiality, integrity, and availability of the information.

5. CONCLUSION

Many organizations use cloud computing technique to store and retrieve their files and data. weakness in any security element, will cause big harm to data and adversely effect on efficiently of work in the organization.

Although cloud computing presents a lot number of benefits to users, it faces a lot of security challenges. Defining exactly data security challenges and suitable solutions is very important to guarantee data integrity. all organization must review all these challenges to overcome the risk involved when the organization used cloud computing. also, security challenges classification and determine its method contribute to reaching the best solution for each challenge.

REFERENCES

[1] Naresh V, B.Thirumala Rao, (2016) A Study on Data Storage Security Issues in Cloud Computing. 2nd International Conference on Intelligent Computing, Communication & Convergence, Procedia Computer Science 92 (2016) 128 – 135. https://doi.org/10.1016/j.procs.2016.07.335

[2] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," J. Internet Serv. Appl., vol. 4, no. 1, p. 5, 2013. https://doi.org/10.1186/1869-0238-4-5

[3] P. S. Suryateja, "A Comparative Analysis of Cloud Simulators," Int. J. Mod. Educ. Comput. Sci., vol. 8, no. 4, pp. 64–71, 2016. https://doi.org/10.5815/ijmecs.2016.04.08

[4] B. T. Rao, "A Study on Data Storage Security Issues in Cloud Computing," Procedia - Procedia Comput. Sci., vol. 92, pp. 128– 135, 2016. https://doi.org/10.1016/j.procs.2016.07.335

[5] N. Khan and A. Al-yasiri, "Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework," Procedia - Procedia Comput. Sci., vol. 94, pp. 485–490, 2016. https://doi.org/10.1016/j.procs.2016.08.075

[6] G. Somani, M. Singh, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing : Issues , taxonomy , and future directions," Comput. Commun., vol. 107, pp. 30–48, 2017. https://doi.org/10.1016/j.comcom.2017.03.010

[7] G. Elavarasan , Dr.S Veni (2015), "A Review on Security Threats and Vulnerabilities in Cloud Computing",International Journal of Engineering Research & Technology (IJERT). Vol. 4 Issue 07, July-2015.

[8] G. Elavarasan , Dr.S Veni (2015), "A Review on Security Threats and Vulnerabilities in Cloud Computing".

[9] International Journal of Engineering Research & Technology (IJERT). Vol. 4 Issue 07, July-2015.

[10] Tripwire Top Cloud Security Threats - https://www.tripwire.com/state-of-security/security-data protection/cloud/top-cloud-security-threats/ (last accessed on Mar, 2018)