iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VIII **Month of publication:** August 2021

DOI: https://doi.org/10.22214/ijraset.2021.37909

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VIII Aug 2021- Available at www.ijraset.com

A Survey of Emerging Threats in Cloud Security

Darshan Bagrao[1], Pratik Tare[2]
[1, 2]*Academic Research Student, Department of Information and Technology, B. k Birla College of Arts, Commerce and Science (Autonomous), Kalyan, Thane, India*

Abstract: ***The original aim of the research was to investigate the conceptual dimensions of cloud security threats and vulnerabilities. Cloud computing has changed the whole picture from centralized (client-server not web-based) to distributed systems and now we are getting back to virtual centralization (cloud computing). Although potential gain achieved from cloud computing but still model security is questionable. . The cloud computing concept offers dynamically scalable resources and so it uses internet as a communication media. This paper proposes survey on emerging threats of cloud and also discussed the existing threat report and their remediation. The result and analysis show that solution of this work will be helpful in summarizing the main security risks of cloud computing from different organizations.***

Keywords: ***Threat, vulnerabilities, model security****.*

I. INTRODUCTION

As technology increases need for the cloud security increases. In general terms for anything that involves delivering hosted services over the internet is cloud and cloud is targeted to provide better utilization of resources. Cloud services delivers application and storage spaces as services over the internet with no cost and to take up much of the work load from the client. We utilize cloud computing services on daily basis. Though cloud based solutions are attractive for their convenience, quick and cost savings data storage, it is fraught with security risks.

Cloud security has become a very vibrant issue in the computing world which make us vulnerable to cybercrimes that happen every day. As per data security is concern technology is not trustworthy, it's affected with threats and vulnerabilities which can lead to misuse and data loss. Threats get access to clouds without legal authorization or disrupt services on clouds in order to achieve specific objectives. Hackers choose most insecure target to steal private and sensitive information for criminal activities by treating their illegal activities as valid instance and gaining unauthorized access to information stored in cloud. To provide more secure services to cloud users it is necessary to understand threats of cloud security.

II. THREATS OF CLOUD COMPUTING

By conducting literature survey various threats and vulnerabilities for cloud computing are identified, these are described as follows:

A. Data Breacher

Data breach can be the main goal of an attack through which sensitive information such as health, financial, private, or confidential data related to a person or organization has been accessed, copied, stolen or used by an unauthorized party.

In 2017, personal data of more than 148 million Americans was stolen and published by hackers. Over 1.4 billion records were lost to data breaches at Equifax.

Remediation

1) Analyze data protection during design and run time.
2) Implementation of strong API access control.
3) Organizations must encrypt and protect data in transit.
4) Implement backup and retention strategies

Fig: Proportion of data beaches and hacking statistics for last few years.

Year	Impacted Data	Quantity
2020	Marriott disclosed hotel guest records	5.2 million
2019	MGM leaked hotel guest records	142 million
2018	Armor's fitness pal's data	150 million
2017	Friend finders sites	412 million
2016	Data of riders and drivers of ubar	57 million

B. Malicious Insider

A malicious insider can be employees, contractor or business associates who can steal the confidential data of the cloud user & easily obtained access to the organizations cloud services at greater levels with little or no risk of detection. These attacks may affect financial value, productivity loss as well as brand reputation of an organization.

In 2018, employee of Cisco former gain unauthorized access to the company's cloud infrastructure and deleted 456 virtual machines used for Cisco's WebEx Teams application, so users couldn't access their accounts for two weeks. Cisco had to spend approximately $1.4 million to fix the damage.

Remediation

1) Enforce security awareness programs and remediate unknown activity in real time.
2) Harden grant access to employees, and set compliance policies.
3) Organizations should automate their processes and use technologies that scan frequently for misconfigured resources.

C. Account or Service Hijacking

An attacker gain access to user's account by phishing, fraud or can spy on their activities, manipulate data and falsify information, redirect them to illegitimate sites. These attack are carried out mostly using the stolen passwords.

At Russia in 1995, Vladimir Levin hacked an accounts of Citibank network and stole $3.7 million .for that he used computer based in London and able to get codes and passwords of customers.

Remediation

1) Multifactor authentication is required.
2) Store or backup your data before it goes cloud.

D. Insecure Interfaces and API's:

For managing and accessing cloud services cloud user uses software interfaces and APIs. The security of cloud services depends upon security of these API's. They are designed to provide accidental and malicious attempts to avoid threat, for that API's need to be protected.

A 2017 report by Red Lock found that 40% of organizations using cloud storage services had accidentally exposed one or more services to the public.

Remediation

1) Use of encrypted keys to access API's.
2) Use good security model and standard API frameworks.

E. Insufficient Identity ,Credential and Access Management

Security threats may occur due to inadequate protection of the credentials and resulted in to stolen credentials. An Unauthorized user can access, modify and delete data, or inject malicious software.

These attacks often occur due to lack of ongoing automated rotation of cryptographic keys, passwords and certificates, failure to use multifactor authentication, weak password use.

Remediation

1) Ues two factor authentication method for secure accounts.
2) Security awareness should be provided to contractors , third-party users and employees.

Threat No.	Threat Name	Possible Vulnerabilities
1	Denial of Service (DoS)	Weak Network Architecture Insecure Network Protocol Vulnerable Application
2	Vulnerable Systems and APIs	Weak API Credentials Key Management Operating System Bugs Hypervisor Bugs Unpatched Software
3	Weak Authentication and Identity Management	Social Engineering Attacks Man-In-The-Middle Attack Malware Infection
4	Shared Technology Vulnerabilities	VM Hypervisor Third-Party S/W Vulnerabilities
5	Lacking Due Diligence	No Auditing Service Level Agreement
6	Abuse of Cloud Services	No Cloud Service Monitoring Service Level Agreement
7	A Lack of Responsibility	Human Negligence Service Level Agreement
8	Ransomware	Infrastructure Platform Application Vulnerabilities
9	Spectre and Meltdown	Hardware Design vulnerabilities
10	Unprotected IoT Devices	Weak Device Management Network and Hardware Vulnerabilities
11	Data Loss	Natural Disasters Simple Human Errors Hard Drive Failures Power Failures Malware Infection
12	Advanced Persistent Threats (APT)	Spear Phishing Direct Hacking USB Malware Network Penetration Third-Party APIs

Fig: Other threats and vulnerabilities of cloud are represented as follows:

III. CONCLUSION

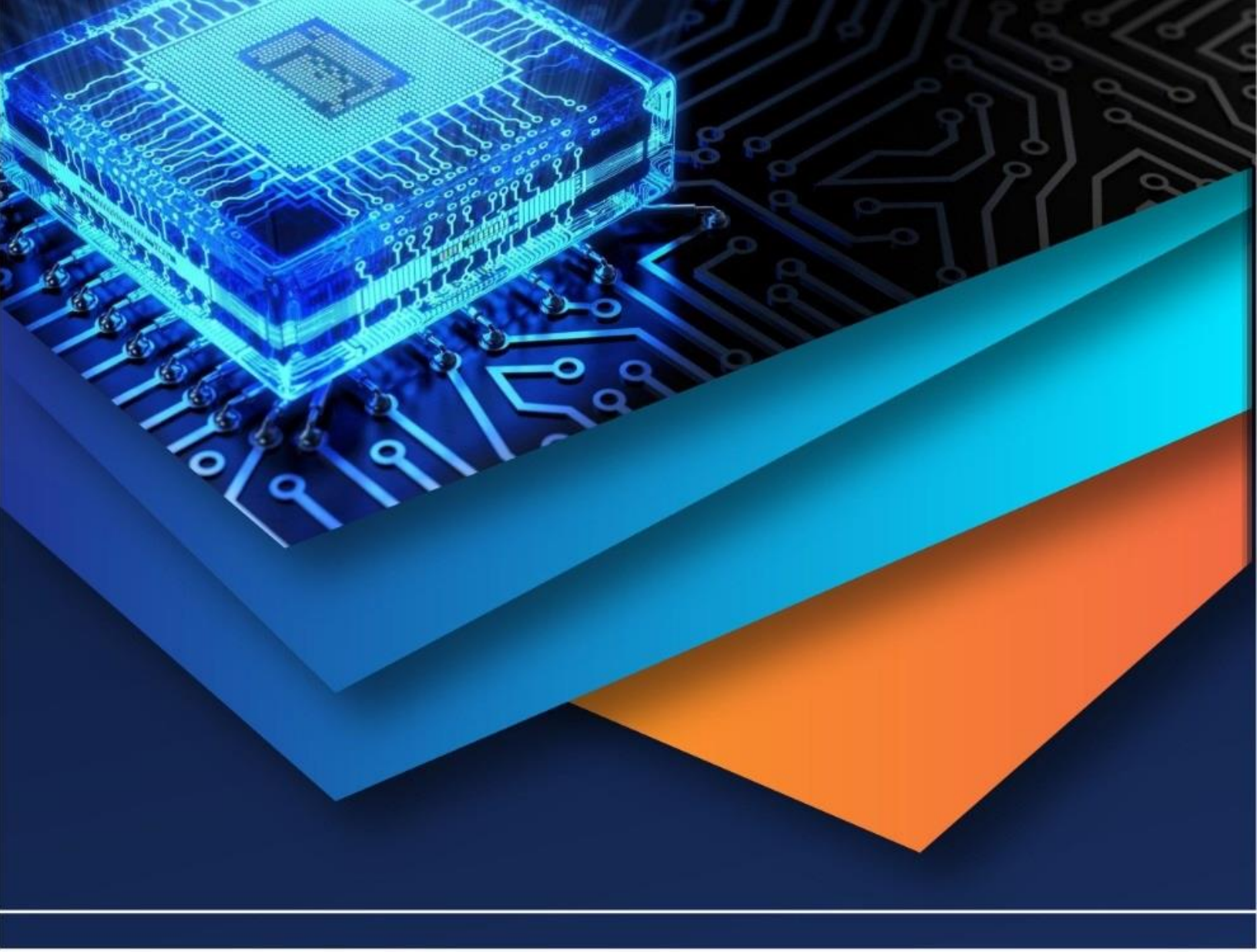
This paper conducted a study to review threads, vulnerabilities of cloud security and listed some of the remediation. Study states that many companies faced this thread and how they overcome from these vulnerabilities. In cloud security end service provider will control access to services. These services hosted on cloud need to protect their network from unauthorized accesses. Vulnerabilities in cloud still exists and hackers continue to exploit these assets. In future I'll continue to studying cloud security threat.

IV. ACKOWLEDGEMENT

The author would like to thank Prof. Swapna Nikale , Department of Information and Technology of B. K . Birla College of Arts, Commerce and Science (Autonomous), Kalyan, Thane.

REFERENCES

[1] https://www.geeksforgeeks.org/cloud-computing/
[2] https://en.wikipedia.org/wiki/Cloud-computing/
[3] http://ijergs.org.managewebsiteportal.com/files/documents/SECUR ITY-64.pdf
[4] http://digilib.stmik-banjarbaru.ac.id/data.bc/Security.pdf
[5] https://www.researchgate.net/International-JournalofApplication.pdf
[6] https://www.researchgate.net/Threats-and-Vulnerabilities-of-Cloud- Computing-.pdf



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY