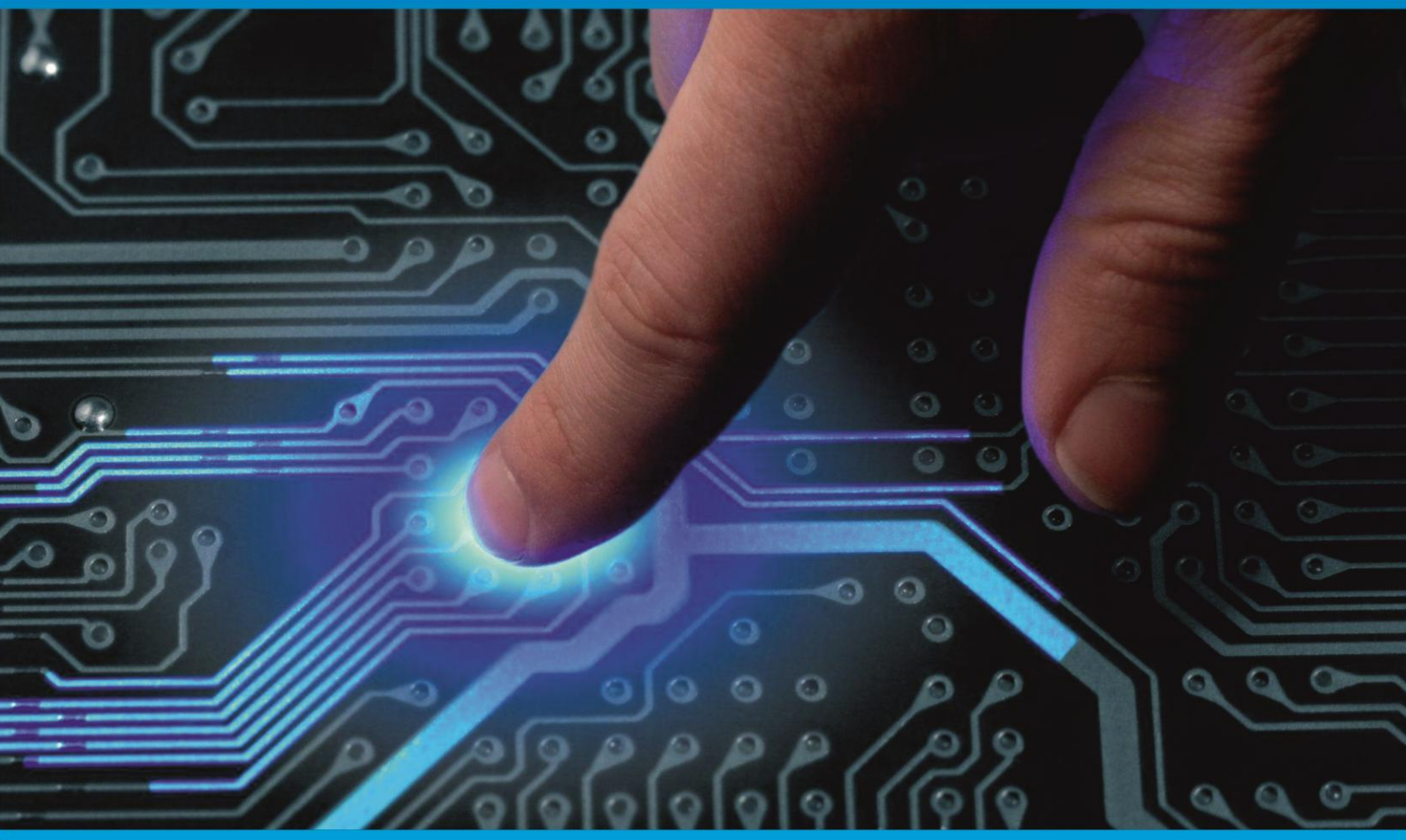
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 4, April 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904120 |

A Study on Cloud Computing Issues and Security Techniques

Raymond Stanley Luciani, Ms. Joy Keren S.

P.G. Student, Department of Computer Science, St. Joseph's College Bangalore, India

Assistant Professor Department of Computer science St. Joseph's College, Bangalore, India

ABSTRACT: Cloud computing is widely used and it takes away a lot of attention of people and the originations, Data over the cloud can be easily stored and accessed any ware around the globe having access to the internet. In this paper we will be discussing some the major attacks which took place in the year 2019 due to the covid-19 pandemic (Corona Virus). Some of the security issue which play an important role in clouding computing and the Like Misconfiguration, Loss of control, Malware Injection Attack, Data breaches etc. Some of the Techniques to secure cloud security and keep it safe from been attacks like Ensure a security Architecture, Secure Information Management, protect data and using various tools to protect and keep the cloud computing safe.

KEY WORDS: Cloud computing, Cloud security, security Techniques, cloud issues.

I.INTRODUCTION

Cloud Computing is the on demand for resource sharing and storage of data over the internet. There are huge data centre built and managed by the cloud server providers in order to provide cloud server to huge organisation, start-up companies and the common people. Cloud computing is widely used in organisation and Academics where the data can be accessed fast and very reliable as it is an open service to all. Cloud computing has a lot of advantage and it is the widely used service in today's world. Since Amazon inverted and started cloud service for their online business and streaming the web series and movies. Slowly all the other organisation like google, Oracle, apple started to use and move the storage and service over the cloud.

In the year 2019, all the organisation moved to cloud and towards online work sources due to the deadly covid-19 virus spreading all over the world. All the organisation faces a major attack during migration, In India,93% of the organisation has faced some ransomware attacks over the internet in order to take data and information for the organisation and they more people from the cybercrime team and monitor the fix the issue. The main reason behinds the attacks on so many organisation which has less cloud security service, where the organisation should have had a proper Authentication for login, and encrypt the password while storing it over the cloud so that no one would be able to view the password and other data without the Encrypted key. The organisation should compliance with the GDPR (General Data Protection Regulation) which will also help the organisation to keep the data safe and protect their cloud from external resources.

The following are some of the major attacks that took place in 2019.

Facebook, In April 2nd Lost around 540000 records which is about 146 GB of data. This was due to a 3rd party application, which exposed 540M records of Facebook users with 22,000 passwords.

Instagram, In May 20th Over 50 million records of their user was exposed to the outside world such as profile Picture, uploaded pictures number off followers and the Bio information, through this information all the linked phone number and email address.

Capital One, July 29th The biggest attack in 2019, The attack damaged over 80,000 accounts, 140,000 social security number and over 1 million Govt. ID number. The attacker was an Amazon software engineer and she used the SSRF (Server-Side Request Forgery) to take the information which was stored over the server.

Auto-clerk, Sept 13thAuto-clerkis hotel reservations management system which happens online and stories all the booking and the transition details online in the server.The details exposed included name, address, phone number and the other sensitive personal data. VPNMentor was the team investigated on this issues and came up this incident.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904120 |

3rd party application, these were some of the major attacks which took place in 2019, and there are more issues and security problem faced by using some off the 3rd party application which pop up on the screen in order requesting for personal information such as name, phone number and email address. The pop up add may look simple that is one off the biggest threat of losing information and allowing the hackers and the attackers to take control over the server and the personal PC and laptops.

III. WE HAVE SOME OF THE SECURITY ISSUE WHICH PLAY AN IMPORTANT ROLE IN CLOUDING COMPUTING

1.Lack of security Architecture, Organisations lacks the implement a proper security Architecture and a protocol to withhold the external attacks during migration process when the business is moving to cloud.
2.Misconfiguration, Misconfiguration is one of the most dangerous thread to the cloud security and server can be attacked very easily if there is a lack in the cloud security Misconfiguration by allowing the attackers to inject virus codes and leak the sensitive details and files of the Origination.
3.Data breaches, Data breaches is the most common issue in cloud computing in the past few years and in the last year 2019 that was the major threat to many of the companies around the world, especially the small start-up companies. Data breaches is that when some of the critically details of the companies or the finically sector, information is let out to the open world or to the public world. The person who has access to these data is a key person who can protect the data.
4.Loss of control, Data in cloud is stored, and the user are unware of location where the data is being stored over the cloud. The cloud server provider can host their server from any ware around the world through internet, if there is any issue or the data is being lost cloud Origination, the user will not know anything about the security mechanism used by the cloud provider.
5.Lack of staff with skills to manage security tools and security software, when business moves online over the cloud services the security staff are mostly not trained on the security software and the policies which is a major thread faced by any Organisations.
6. Data loss, as there are multiple tenants, data integrity and others data safety features and still at times the data is not provided with proper and required safety.
7.Internal attacks, Internal attacks are one of the most difficult to prevent from any kind of damage or losing of information, this types of attacks are done within the Origination by the employee and the contractor who are appointed by the Origination, where they have the access to the security access and they might change them and allow external sources to attack the service or make changes to the server to affect the company's assets.
8.Interfaces and API's,The Interfaces and API's are the most exposed to the outside world, where It connects the user to access and data stored in the cloud. Interfaces and API's are the common tool for the attacks to perform suspicious activity on the cloud.
9.Malware Injection Attack, In Cloud there are a lot for transfer between the cloud service provider and the user. Malware Injection Attack are basically done to cake control of the user data and the user information. Hackers will implement interfaces servers with a set of Malware codes in to the user VM and if this process is done the hackers can take control of the could server.
10.Limited cloud usage visibility, this is the most common security thread in the cloud services, where the Origination won't be able to visualize and check in which part of the cloud service the data can be kept safe and in which part of the cloud is unsafe within the origination. If the employee has an access to the security with any without permission and without any security staff, then there is a high risk where the security is unware of this access. There can also be an external resource accessing the cloud with stolen information.

IV. TECHNIQUES TO SECURE CLOUD SECURITY AND KEEP IT SAFE FROM BEEN ATTACKS.

1.Ensure a security Architecture
An Origination should always have a proper cloud security architecture and strategy, which is very important in protecting the cloud and the most required element of cloud security. The Origination should come up with a security Architecture which goes along with the business goals and protest the data, Test the module and framework build multiple times with various attacks tested and record the performance, As the cloud world is getting updated day by day, the module should be updated with the required features. Continuous monitoring the module and how well the module can protect the data from attackers. As this might be a little expensive it can help an Origination to keep the data save over the cloud.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904120 |

2.Avoid Misconfiguration

Misconfiguration and inadequate change control is one of the most of the major issue, this can be carried out by any security staff by mistake or unknowingly (lack of training). Configure IP address with the company ranges and setting required by the company, always best to use an automation and advance technologies while configuring security setting, where it can perform the configuration setting and also scan for any Misconfiguration if there and available and restore the required configuration.

3.Overcome Data breaches

Encryption of data can protect the data from data breaches, they would require a robust technique and a tested incident response from the cloud provider is there any issues, the prevention of data breach should be from both user and the cloud provider. Patching and updating Data breaches software when there are updated, highly encryption process is required for the data, multi-factor authentication while logging in. Training the employee on the security techniques to avoid attacks.

4.Secure Information Management

In this technique, the cloud computing it will know the where the data is stored in a central repository. It monitors all the information which is running and keeps track and it is sent to the SC (security console). Where all of this is managed by a human been (Admin) in the cloud provider company. He also has the access and control to review the setting on the account and take action if there any error and alert notified to him.

5.Staff training on security

This is one of the main task which should be carried out by any company, where the staff should always have more training on the updated security tools and the techniques used by the company, this will help people to react and figure out if there are any unauthorized access on the service and solve the issue with less time and in the best and the required steps where it will increase the security level in that company. increasing knowledge on the security tool and technique and in the security level in the cloud.

6. Protect data

Data can be destroyed and damaged in many ways, cloud providers can follow the best technique to protect the data, Keep the physical storage (data centre) should always be located in a less temperature location, Control the flow of request, continuously back-up the data, Use DLPS data loss prevention software, Monitor the account behaver. Regular check for data environment if there are at any level of risk.

7.Provide requires access to employee

Monitor the employee access behaviour, conduct frequency training on the security in their specific roll. Use the required UAM (User activity monitoring) for the employees Regularly audit the roll of each employee, restrict employee access to critical systems if there are not authorised to that specific system.

8.Reliable interfaces and API's

Interfaces and API's should always be user friendly as the connect the user and the cloud services to perform specific tasks, implement good APIs its simple and is also strong after the development stage, where it should be tested multiple times and with all level of attacks, use high API key to avoid risk and attacks. Consider an open API framework such as CIMI.

9.Malware Injection Attack

Staff or the user should avoid phishing emails, where those specific contains a loss of links by click on that link the attacker can gain access to the system or the cloud service. It is required for the staff to look into odd login in a specific network in unusual working hours would indicate suspicious activity and it would be easy to look into the issue. Keeping track of the network and who is using the network can avoid these kinds of attacks. We can also use Hypervisor to manage the issue and a IDT (Interrupt Descriptor Table) can be used as a integrity check for the process.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904120 |

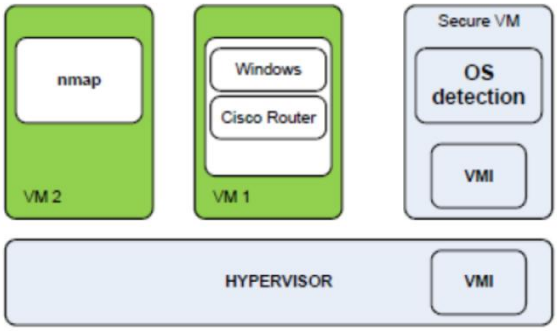


Fig 1.1 Hypervisor

10.Limited cloud usage visibility

Complete Cloud Visibility with Traffic Mirroring The best way is to continuously inspect and monitor the incoming and outgoing traffic It is very check the transfers from both sender and the receiver side which will avoid risk thread which is coded inside the data packet which can affect the cloud. There are many tools which can be implemented in this process, so it would be more help full to monitor the traffic, these tools will not affect the performance or the Architecture unless they manually configure changes.

Garland Prisms is one of the tool which is used for cloud usage visibility, they automatically take care of the dynamic workload, packets, maintain control over the cloud.

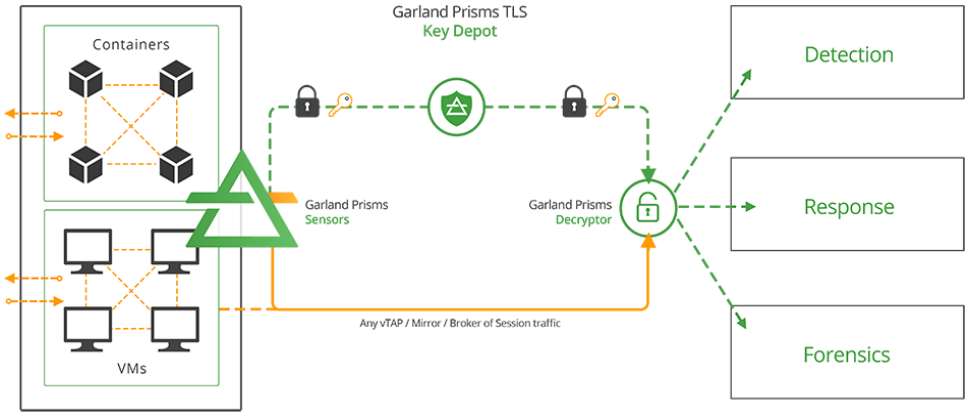


Fig1.2 Garland Prisms

By guaranteeing 100% packet capture from your clouds, you're able to satisfy your virtualized security strategy- Garland Prisms

V. CONCLUSION

In this paper we describe some off the security issue, attacks although there are various attacks and issues faced by cloud computing in this paper we have taken some of the major attacks took place in the year 2019. Some of the cloud attacks and the ways the prevent it and make cloud more secure for the feature. Recommendations, implementation of the new privacy regulations to keep their cloud services safe like The General Data Protection Regulation and California Consumer Privacy Act, Cloud Security Alliance (CSA) and NIST or any other Consumer Privacy Act which will increase the security. Increase control to investigate if there are any security issue and damage as this was the major effect. Encryption of data (which is more common, and which is not followed). Use DDC (data discovery and classification) to investigate what kind of data should be moved towards the cloud and what kind of important data

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904120 |

should kept on the ground office. Implementationof security monitoring application in the organisation to keep the cloud service safe and inform the staff to the small malfunction.

REFERENCES

1.A Survey on Cloud Security Issues and Techniques –Garima Gupta, P.R. Laxmi, Shubhanjali Sharma (2011)
2.Akhil Behl (2011), Emerging Security Challenges in Cloud Computing (An insight to Cloud security challenges and their mitigation).
3.Cloud Computing Challenges in a General Perspective, Ngo Yang Chong, University of Warwick Coventry, United Kingdom (2019)
4.Security Techniques for Data Protection in Cloud Computing, Kier Jakimoski, FON University (2019)
5.D. W. Chadwick and K. Fatima, "A privacy preserving authorisation system for the cloud", Journal of Computer and System Sciences (2012).
6.Cloud Computing Security Issues, Challenges and Solution, Pradeep Kumar Tiwari, Dr. Bharat Mishra (2012)
7. A survey on security challenges in cloud computing: issues, threats, and solutions, Hamed Tabrizchi, Marjan Kuchaki Rafsanjani (2020)
8.https://cyber attack: 93 percent organisations reported attacks on cloud infra in last one year: Sophos, Telecom News, ET Telecom (indiatimes.com)
9.https://The Biggest Cloud Breaches of 2019 for 2020 - (lacework.com)
10.https://www.lacework.com/top-cloud-breaches-2019/
11.https://www.csoonline.com/article/3043030/top-cloud-security-threat.html
12.https://purplesec.us/resources/cyber-security-statistics/
13.Cloud Security Challenges in 2020 (cloudsecurityalliance.org)
14.https://medium.com/@IDMdatasecurity/main-cloud-security-threats-9deb6351922
15.https://www.netwrix.com/2019cloudsecurityreport.html
16.https://www.netwrix.com/2018cloudsecurityreport.html
17.https://www.netwrix.com/2016cloudsecurityreport.html
18.https://www.itworldcanada.com/blog/is-loss-of-control-the-biggest-hurdle-to-cloud-computing/95131.
19.https://www.govtech.com/blogs/lohrmann-on-cybersecurity/the-top-20-security-predictions-for-2020.html
20.(12247) Cloud Computing Tutorial For Beginners | What is Cloud Computing | AWS Training | Edureka - YouTube
21. eSentire | Security Operations Center (SOC) | Security Operations

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details