International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 8 Aug. 2022, pp: 58-62 www.ijaem.net ISSN: 2395-5252

Cloud Computing –Security

Rutuja S. Gangane & Gauri N. Nebhwani

Submitted: 01-08-2022 Revised: 02-08-2022 Accepted: 08-08-2022

ABSTRACT:-
The cloud computing is a new computing model which comes from grid computing, distributed computing, parallel computing, virtualization technology, utility computing and other computer technologies.
Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. Large clouds often have functions distributed over multiple locations, each location being a data center.

I. INTRODUCTION

Cloud Computing Security Cloud computing security refers to the security enforced on cloud computing technology. In simpler terms, cloud security provides support and security to the applications, infrastructure, and procedures and protects data from vulnerable attacks.

Cloud-based security platforms also work on a private model that consists of a private cloud, isolating the unauthorized data access from the clients ensuring protection from shared security platforms Cloud computing security also works on securing data identity by deciphering the encrypted data.

Cloud computing security refers to the security enforced on cloud computing technology. cloud security provides support and security to the applications, in frastructure, and procedures and protect data from vulnerable attacks.

Cloud security risks

- Data Loss
- Spectre & Meltdown
- Denial of Service (DoS) attacks
- Account hijacking

Security Concerns in Cloud Computing

Unauthorized Access

Cloud computing is very useful for its ability to provide access to all of your team membersthrough a simple internet connection. However, this is also why it can be a liability because people from outside your company can also access the entry points.

Misconfigured Security Settings

This can be a great asset when used correctly. There is a lot of room for customization in your cloud security settings. However, it can also be a liability when the settings aren't properly configured.

Insecure APIs

Application User Interfaces (APIs) are a means of interacting with the cloud computing system. They also help users to customize their cloud computing system

Data Breaches

This transfer of information creates opportunities for cybercriminals to intercept it.
Data is constantly in flow between users and the cloud-based system. [3]

Data Leaks

This can be done accidentally or intentionally, but it's potentially damaging either way.Cloud-based computing systems make it very easy for one member of your organization to share information with another member.

Malware

A malware attack involves cybercriminals uploading their own code or scripts into your cloud \ servers. These functions infect your system and runjust as any other valid software would run.

Denial of Service Attacks

A denial of service (DoS) attack doesn't aim to access your sensitive information. The goal is to create a situation where your system is unavailable to the users that need it. [3]

Insider Threats

Cloud computing systems make oversight more difficult because of how the information is shared throughout the organization.
This can be performed by triggering a crash or sending so much traffic to the system that it becomes overwhelmed.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 8 Aug. 2022, pp: 58-62 www.ijaem.net ISSN: 2395-5252

Privacy and privacy assessment

Privacy is an important consideration in cloud computing. It is a systematic process for evaluating the possible future effects that a particular activity or proposal may have on an individual's privacy. As actual or perceived privacy weaknesses will impact legal compliance, data security, and user trust. It focuses on understanding the system, initiative, or scheme; identifying and mitigating adverse privacy impacts; and informing decision-makers.[2]

Operating system security

An operating system (OS) allows multiple applications to share the hardware resources of a physical system, subject to a set of policies. Data brought into the system may contain malicious code; this could occur via a Java applet, or data imported by a browser from a malicious Web site.

A critical function of an OS is to protect applications against a wide range of malicious attacks such as unauthorized access to privileged information, tempering with executable code. Such attacks can now target even single-user systems such as personal computers, tablets, or smartphones.

Cloud Characteristics

Cloud computing has some key characteristics that depict their features of similarity and differences from conventional computing operations.

- On-demand Self-service:
- Broad Network Access:
- Resource Pooling or Provisioning:
- Rapid Elasticity and Scalability:
- Measured service or Utility-based pricing: Location Independence
- Cost Effectiveness:
- Multi-tenancy:

Cloud development models

Private model:

The private model is a developer environment in which the entire cloud-based computing infrastructure is dedicated to one user organization.

This cloud-based developer environment can be hosted by the using organization or by a vendor that offers private virtual hosting services. In a private virtual environment, the using organization usually manages the operations within the cloud-based developer environment.

Public Model

The public model is a developer environment in which a set of predetermined infrastructure is shared among a group of tenants. Public environments are hosted by vendors that often provide both public and private environments. The hosting provider maintains the infrastructure, installs updates and patches, and manages the application software as part of the service. [2]

Community Cloud Model

The community model is a relatively new concept for cloud-computing environments. Community clouds offer infrastructure that hosts share among user groups that are working on similar projects or that have the need to collaborate with each other. Third-party service providers host community clouds. [2]

Security Architecture of Cloud Computing:

A cloud security architecture (also sometimes called a "cloud computing security architecture") is defined by the security layers, design, and structure of the platform, tools, software, infrastructure, and best practices that exist within a cloud security solution.

IaaS Cloud Computing SecurityArchitecture

Infrastructure as a service architecture has majorly security and networking tools to protect the network of data. Hear the application programming interface impact is high rather than the other. Even though the cloud service provider's (CSP) provides security for the infrastructure, the remaining Security will be provided by Network tools like network packet brokers (NPB).

The attributes of IaaS Cloud Computing Security Architecture are:

- Segmentation of the network will be in practice.
- Virtual Network tools are stored in the cloud.
- Virtual firewalls and web applications were preferred to use. It helps to prevent malware or threats.[1]
- Optimum utilization of Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS).
- Virtual routers are also introduced.

SaaS Cloud Computing Security Architecture

Cloud access security brokers play a vital role in this Security model. As the name itself specifies that the Cloud security architecture majorly monitors the software and the data can be accessed with the help of the Internet's connection for the management. Management needs to negotiate with the CSP team to maintain proper security based on the legal contract between the

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 8 Aug. 2022, pp: 58-62 www.ijaem.net ISSN: 2395-5252

security team and the management.
The features of SaaS Cloud Computing Security Architecture are:

- Usage of multiple logs is highly prioritized.
- IP restrictions were strictly followed to maintain the security concerning management also.
- Application programming interface gateways are also used In This Cloud computing security architecture plan.[1]

PaaS Cloud Computing SecurityArchitecture:

Cloud security reference architecture for Paas majorly depends on the cloud security providers. The platform as a service model can be defined as the deployment of applications that can be done by considering the capabilities of the host and underlying software and hardware. But it doesn't consider the cost and complexity of buying those applications. As we already know that the applications can be taken care of by the management, the remaining data needs to look after by CSPs.
Features of PaaS Cloud Computing Security Architecture are:

- Security in cloud computing is an important concern.
- Data in the cloud is necessary to be stored in encrypted form. It restricts the client from accessing the shared data directly. For this purpose proxy and brokerage services are necessary to employ.
- Encryption helps to protect transferred data as well as the data stored in the cloud. Encryption also helps to protect data from any unauthorized access, but it does not prevent data loss.[1]

Key Elements of a Cloud SecurityArchitecture:

- Security at Each Layer
- Centralized Management of Components
- Redundant & Resilient Design
- Elasticity & Scalability
- Appropriate Storage for Deployments
- Alerts & Notifications
- Centralization,Standardization, &Automation

Planning of security

In security planning, before deploying a particular resource to cloud there is a need to analyze different aspects of the resources which are as follow:

- Select resource which requires to move to the cloud and examine its sensitivity risk.
- The cloud service models i.e. IaaS, PaaS and SaaS are necessary to be considered for security at different level of services.
- The cloud types, i.e public, private, community, hybrid also need to be considered.
- The risk in a cloud deployment generally depends on the types of cloud and service models.[3]

Security Boundaries

- A specific service model defines the boundary among the responsibilities of customer and service provider.
- The boundaries between each service model are defined by Cloud Security Alliance (CSA) stack model.
- Following diagram shows the cloud security alliance (CSA) stack model.

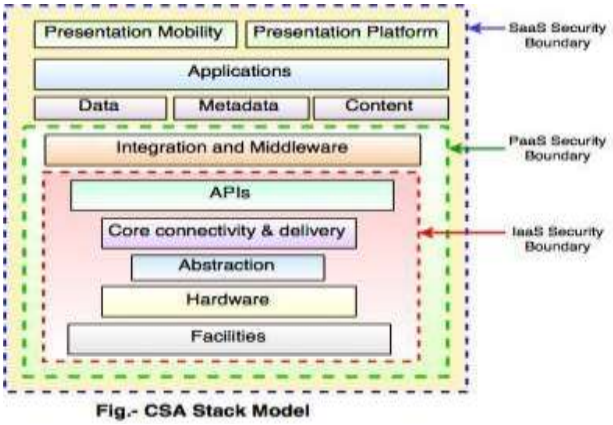


Fig.- CSA Stack Model

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 8 Aug. 2022, pp: 58-62 www.ijaem.net ISSN: 2395-5252

Data security in cloud

Data security in cloud is an important concern because all the data is transferred usingInternet.
Following are the mechanisms for data protection.

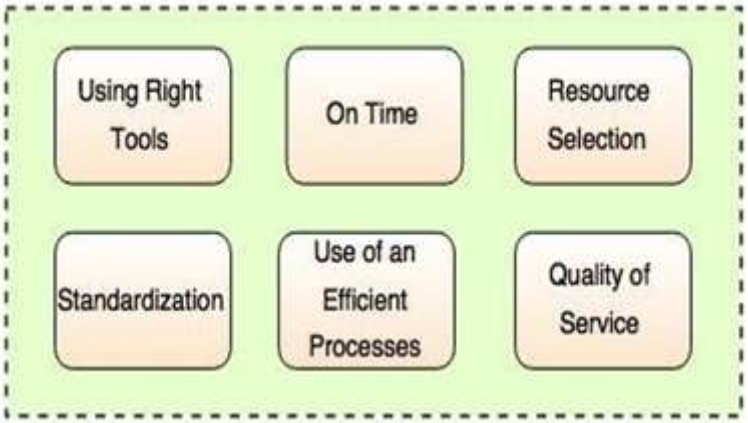
I) Access Control
ii) Auditing
iii) Authentication
iv) Authorization

Operations of Cloud Computing:

- The operations can be accomplished using a web application or mobile applications.
- In cloud, various operations can be performed.The major ones of them are shown in following diagram.

Managing Cloud Operations

There are different ways to manageeveryday cloud operations.
These ways are shown in following diagram:



- It is necessary to employ right tools and resourcesto perform any function in the cloud.
- It is mandatory to do all the things at the righttime and at the right cost.
- It is necessary to select appropriate resources foroperational management.
- The process must be standardized and automatedto manage repetitive tasks.
- It should use an efficient process which eliminatesthe waste of efforts and redundancy.
- It is necessary to maintain the quality of service toavoid the re-work.[4]

II. CONCLUSION:

Cloud-based computing has gotten cheaper to use in recent years, and businesses are rushing toget cloud-based software applications as a result. Itjust makes sense that applications that are designed to run in a virtual environment be developed in one. However, the cloud-based developer modelthat you choose will impact your IT security and the way that your teams conduct Devops.

Cloud computing security refers to the security enforced on cloud computing technology. In simpler terms, cloud security provides support and security to the applications, infrastructure, and

procedures and protects data from vulnerable attacks.

REFERENCES

[1] Cloud Computing Theory and Practice writtenby Dan C. Marinescu.

[2] Cloud Computing–A Comprehensive Definition I. Ahmad, H. Bakht, U. Mohan

[3] Online-https://www.tutorialride.com/cloud-computing/security-in-cloud-computing.htm

[4]Online-https://www.cdnetworks.com/cloud-security-blog/5-key-cloud-security-challenges/