Cloud Computing Security threats and challenges - A Systematic Study

*[1]Dr. B.Jagadhesan, MCA. MBA. M.Phil., PhD, [2]M.Gomathi.
[1]Associate Professor & Head of the Department of Computer Science,
Dhanraj Baid Jain College, Chennai, India,
Email:bjagadhesan@gmail.com
[2]M.Phil Scholar Department of Computer Science
Dhanraj Baid Jain College,Chennai, India,
Email:gomathimuthu2397@gmail.com

ABSTRACT

Cloud computing has become one of the interesting topics in the IT World today.Cloud computing resources has increased their greater reliability,massive scalability, and cost per their usage All these has increased the businesses and individuals to work on the cloud more. In the recent years, cloud computing has grown considerably in the Information technology. Now the number of cloud uses and organizations has increased in the cloud. As well as the Demand of cloud computing raises,the major concern is on its security. Security issues is the major concern facing in the cloud computing. It makes complications in data privacy and data protection. To avoid this people have to be aware of the data breaches in cloud environment. This paper highlights issues related to cloud computing and precaution measures to avoid those threats.

Keywords- Cloud computing, cloud computing models, Threats, Challenges.

I.INTRODUCTION

Cloud computing provides a major change in the way of storing the information and run applications. Cloud computing allows us to access applications and documents anywhere in the world. In the traditional computing method, programs and documents everything shared from one computer to another computer. But with the cloud computing, programs ,documents anything can be shared and stored anywhere in the internet and it can be accessed through the internet. Understanding the cloud computing and its features peoples were moved from the traditional ways to cloud computing services. Thus cloud is more powerful and accessible it can connect through thousands of computer together this can't be achieved by a single pc and also we can store our data from multiple repositories and it can be accessed through anywhere in the world in the real time.

Cloud Architecture is a massive network of servers, computers and individual pc's are interconnected in a network. Cloud computing consists of the different types of computing services which are delivered remotely to the clients via the internet. Cloud provides two types of services they are cloud computing service models and cloud computing deployment models. Those service models are Software as a service, Platform as a service, Infrastructure as a service. These Services are using for different purposes for IT peoples. Next cloud computing deployment models There are four models They are public ,private, community and hybrid. These models are used based on the Infrastructure for the user environment. These deployment models vary on the controls of the infrastructure. Cloud computing provides us lot of advantages which includes Speed and Efficiency Since there are also a host of potential threats in cloud computing. Cloud computing security threats are data breaches, misconfiguring cloud storage, Insecure API and DDoS attacks.

II.Cloud Computing Models

II. a Public Cloud

In Public cloud, Service providers make their cloud services and resources available to the public commonly which also includes storage capabilities, applications or virtual machines. Some of the public cloud providers offer free services to the public. Cloud Services are also available for the individual users, like the organizations and prices are depends on the user's resource needs. Public clouds are useful for both Individuals and Organizations.

Public cloud allows organizations to use large scale of resources this can't be achieved easily with the on-premises data centre. When using regular hardware and maintenance in organizations .When business sector grows well then it is difficult to set up large arrangement but Cloud makes it well even when it grows well.Usually,when organizations using cloud-based services and applications they doesn't require hardware and maintenance in a traditional manner.

This public cloud strategy offers organizations to grow their development scale without and high costs. Service Providers such as Amazon Web Services, Google Cloud Platform and Microsoft Azure offers organizations to for the resources which they had use. This protects the organizational budget and supports their growth as well. Using Cloud Organizations will no longer worry about the Installations and maintenance . Instead of using Large scale hardware ,now they can use cloud -hosted services which will make as update to enhance the business well.

II. b. Private Cloud

Private cloud computing model is used by single business entity peoples. Compare to other cloud computing models, private cloud providers provide virtualize computing environments. Private cloud deployment provide the control to their organization itself. Because the private cloud is only accessible to the single business entity. This Private cloud strategy can be provided by both Exclusive network and also through the virtual private clouds. In the network providers, hardware and storage configurations are maintain by a individual network when coming to virtual private clouds they are paid for on a rolling basis.

Private Cloud computing offers flexibility, cost savings, security, and control benefits in services. These benefits are particularly valuable for businesses with predictable workloads or customization requirements, and businesses in regulated industries.

IT industry will achieve benefit of the private cloud environment is the Flexibility, guaranteed resource availability, strong security and regulatory compliance and also majorly Cost optimization. Different types of cloud computing were using Virtualization technology .Nowadays, Virtualization also provides and enhance the private cloud users with more advanced utilization.

II. c. Hybrid Cloud

Hybrid Cloud is the combination of both public cloud and public cloud In hybrid cloud, data and applications can be shared between them. Hybrid cloud computing not only allows companies to scale computing resources, it also eliminates the need to make large capital expenditures. Hybrid cloud is the best platform for providing all the benefits they include flexibility, scalability and cost efficiencies and with the lowest possible risk of data exposure.

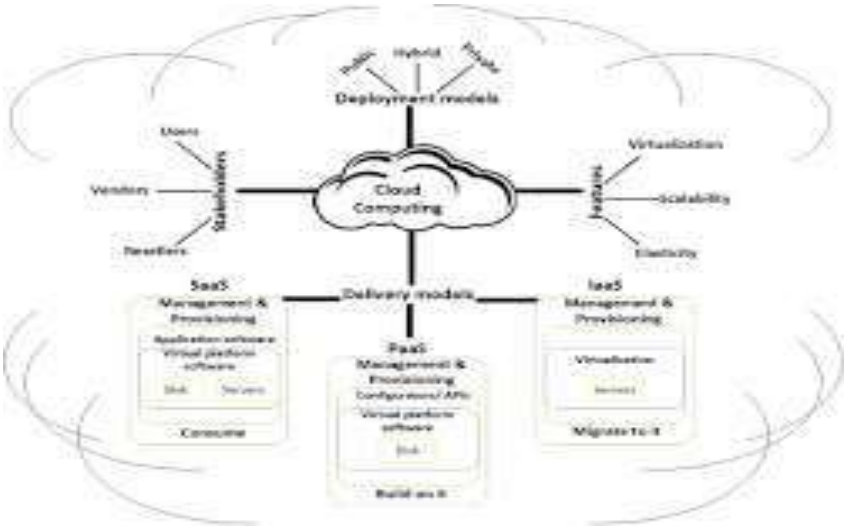
Hybris cloud computing provided the advantage of both the private and public cloud advantages This Hybrid cloud services are a powerful resource for organizations which gives the business control on their private data. Organizations can use public data available to everyone and private data as private ,which makes the management efficiently use of the client data and employment data as well. A hybrid cloud relies on a single plane of management, unlike a multi-cloud strategy wherein admins must manage each cloud environment separately.

II. d. Community Cloud

Community Cloud is different from the other three clouds because it is a hybrid form of private cloud. They are multi-tenant platforms that enable different organizations to work on a shared platform.

The main intend of this Community cloud is to allow multiple customers to work on joint projects and applications that belong to the community, where it is necessary to have a centralized cloud infrastructure. Community Cloud is a distributed infrastructure that solves the specific issues of business sectors by integrating the services provided by different types of cloud solutions.

Community Cloud computing allows its users to identify and analyze their business demands better. Community Cloud may be hosted in a data center, owned by one of the tenants, or by a third-party cloud services provider and can be either on-site or off-site.



III. Cloud computing service models

The Cloud computing service models thereof generally conveys about the Cloud service delivery. These models vary accordingly by their service and infrastructure. they are also known as SPI Model. which means software, platform and infrastructure

III. a. Software as a Service (SaaS)

Software as a service makes the people to work on software on real time instead of installing it for a huge cost.This SaaS will be provided by the third party vendor.

SaaS allows the users to pay for the rent or subscribe to a software which they need and execute it online, rather than purchasing it to install on to their computers. This Cloud services provider installs, operates, and maintains the required type of software application on behalf of the company. Which reduces the installation and maintenance costs typically associated with IT platforms or

Most of the SaaS applications run directly through our web browser, which means they do not require any downloads or installations on the client side. SaaS provides number of advantages for companies and also for employees by reducing the cost and work it reducing the installation, management and also downloading the software. By using SaaS mainly reducing this technical staffs by spending more times for execution instead of maintenance and installation.

III.b .Platform as a Service (PaaS)

Platform as a service is oneof the important cloud computing model which allows the third party provider to delivers its hardware and software tools to uses over the intent. Main intend of this service is to host the hardware and software on its own infrastructure. This PaaS helps the clients to provide platform which helps the people to avoid build and maintain the infrastructure like software development process and also which leads to faster development and delivery of applications.

PaaS allows the users by providing new languages ,different types of operating system ,databases and other developing technologies quickly they are providing the supporting infrastructure. IT makes users to work faster ,easier and also by upgrading tools.

III .c. Infrastructure as a Service (IaaS)

Infrastructure as a service allows the virtual computing resources to the user through the internet. IaaS is one of the main components of cloud computing work along with the (SaaS) Software as a service and (PaaS) Platform as a service. This IaaS cloud service model helps the users to avoid the cost and complexity of purchasing and managing their own physical servers Instead of managing the Infrastructure with this technology Now users can concentrate on the installing ,configuring and managing their software.

With the IaaS, Now the cloud buyers rent a space in the virtual data centre of the IaaS provider and they get the access of using the virtual data centre through the internet. The cloud service providers enable the users to rent the virtual servers and storage to work them together. While renting the cloud IaaS provider, users are essentially renting hardware along with the provisioning software that automates it.

IV. Security Threats in cloud computing

The Threats in cloud security can vary by their cloud deployment models and by the usage of the cloud in Internet.There are number of security threats is cloud computing. This table provide the overview of the threats by their cloud security model.

Threat	Description
Data Breach	A Data Breach can be intentional or unintentional incident which will releases the secure and private confidential information. This can also be done by the cybercriminal by hacking the database.
Data loss	In Data Loss data/application will be corrupted, deleted or even make as unreadable by the user This will usually happen when the data or application no longer used by the owner.Data loss literally known as Data leakeage this can also be occurs due to the technology fails or the computer freeze or by the backup files are lost.
Insecure API	Usually API are provided by third party applications for web and cloud services. This threat will be done by the attacker with access to the key and cause a deniel of service when the service providers are not aware of it.
Misconfigured Cloud Storage	Cloud misconfiguration occurs when we missed to create a storage gateway to access data and also misconfiguration will leads to vulnerable attacks and API's under risk.
DOS Attack	a **denial-of-service attack** (**DoS attack**) is a cyber-**attack** in which the attacker seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

IV. a. **Data Breach**

Data Breach is one of the cloud security risk. In Data Breach, Information is accessed and extracted without the authorization of the user. This will result in a data leak. Security Breach occurs due to the attacker who gains unauthorized access to an organization. This will

affect the protected data and systems. Data owners express security concerns to outsource their data to public cloud, to avoid this data breach Multi-factor authentication is the security component. This will provide additional password to their regular password and user gets a disposable key on their private device when someone tries to hack it the account will automatically locked down and also it sends a notification message to the user while attempting the break down.

IV. b. **Data loss**

Data is being intentionally or accidentally deleted or overwritten by a user or an attacker. Data losse are occur due to dynamic databases and also occur problems on the cloud providers side Data loss can be prevent using backups.Keep on back up the frequent databases For this we need a schedule for the operation and clear delineation of what kind of data is eligible for backups and what is not. Use data loss prevention software to automate the process of Data loss.

IV. c. **Insecure API**

A Cloud Provider Application programming Interface will interact the users to attain cloud provider service to the end user , This makes the cloud customer with the ability of the cloud to use and access the cloud resources on the cloud computing platform. This occur due to anonymous access, lack of access monitoring. To avoid the problem of Insecure API by using General system security audits, Secure Socket Layer/Transport Layer Security encryption for data transmission and also Multi-factor Authentication to prevent from the unauthorized access .

IV. d. **Misconfigured Cloud Storage**

Cloud misconfiguration is a setting for cloud servers that makes it vulnerable to breaches. This misconfiguration occurs due to following reasons when confidential data is left out in the open and requires no authorization. when an unauthorized person unintentionally gets access to sensitive data and Default cloud security settings of the server with standard access management and availability of data. This can be prevented by Double-checking the cloud security configurations upon setting up a particular cloud server. When it seems obvious, it gets passed by for the sake of more important things like putting stuff into storage without second thoughts regarding its safety.

Use specialized tools to check security configurations. one of the third party tools like CloudSploit and Dome9 can check the security configurations before on time and identify possible problems and ensure .

IV. e. DoS Attack - Denial-of-service attack

A denial-of-service attack (DoS attack) is a cyber-attack which the unknown perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely. The purpose of the denial-of-service attack is to prevent the users from accessing the applications or disrupting its workflow. DoS is a way of messing with the service-level agreement (SLA) between the company and the customer. This intervention results in damaging the credibility of the company. The thing is - one of the SLA requirements is the quality of the service and its availability. There are two major types of DoS attack One is Brute force attack from multiple sources (classic DDoS), and the other one is More elaborate attacks targeted at specific system exploits (like image rendering, feed streaming, or content delivery) During a DoS attack, the system resources are stretched .

Lack of resources scale causes that multiple speed and stability issues across the board. Sometimes it means an app works slow or it simply cannot load properly. For users, it seems like getting stuck in a traffic jam. For the company, it is a quest to identify and neuter the sources of the disruption, and also increased spending on the increased use of resources. To avoids the DOS attacks these system are used they are Up-to-date Intrusion Detection System. This system can be able to identify anomalous traffic and provide an early warning based on credentials and behavioural factors for the users. It is a cloud security break-in alarm. Firewall Traffic Type Inspection features allows to check the source and destination of incoming traffic, and also assess its possible nature by IDS tools. This feature helps to sort out good and bad traffic and swiftly cut out the bad. One of the critical goal of the Dos is to consume Bandwidth is Source Rate Limiting. Blocking the IP address is also the source of attack but it used to help to keep the situation under control once it is attacked

V.Conclusion

Cloud Computing plays a major role in today's world and provide number of benefits for its users in the realtime. In this paper we have seen about cloud computing deployment models and the cloud computing service models , they are differed depending on their model and its usage. Cloud is providing enormous number of facilities to the people .Since, cloud having major security concerns.This paper major intention is to know how to avoid those security concerns These can be overcome due to some of the techniques like Multi factor authentication,Backups and etc. For this people have to first understand about the challenges and threats which are existing while using cloud computing and take precautions depend upon the Security of the data.

References:

[1] Dhanammashankarjagli - International journal of engineering research and applications · june 2017.

[2] Adnaanarbaazahmed, dr.m.i.thariqhussan- -International journal of advanced research in computer engineering & technology (ijarcet) volume 7, issue 4,april 2018, issn: 2278 – 1323.

[3] Florin ogigau-neamtiu - The regional department of defense resources management studies, brasov, Romania.

[4] Michael Miller-"Web-Based Applications That Change the Way You Work and Collaborate online"