WORLD OF CLOUD COMPUTING SYSTEM PROTECTION FOR THE NETWORK SECURITY ENVIRONMENT SYSTEM

Prof.Arpita Singh
Mail id:-singharpita2009@gmail.com
(Inmantec Institution, Ghaziabad)

ABSTRACT

Protecting digital information from unauthorised access, curruption, or theft throughtout all stages of its lifecycle is the concept of data security.Big data and cloudcomputing continue to face a number of challenges when they become more widely used in e-commerece.In the framework of cloude computing, this article mainly discusses about security of big data based on cloud Environment. Many businesses need efficient methods to store and process enormous quantities of data.Scalable resources and considerable financial benefits in the form of reduced costs of operation are provided by cloud computing as an enabler.This paper is discuss on the essential problem of security of e-commerce in information and could computing storage. The primary objective of this research is to provide a secure environment for online transaction.

The Internet has played a significant role in facililitating the exchange of resources and data as well as serving as a serving as a bridge to link individuals world wide as a process of globalisation has intensified.The processing and sharing of data have become faster becouse to the development of cloudcomputing.But as new technologies have emerged ,so too have new security dangers.As a result, in the context of cloud computing ,the issue of computer network security is also receiving more attention.This paper discusses the crucial issue of world commercial information and data storage security.

Key word:

Platform as a service (Paas), Software as services (SaaS), Instrastucture as a service (IaaS), Denial of Facilities, Cloud

1. Introduction

Cloud computing has advanced rapidly during the last few years.Through the internet, cloud computing provides customers with a variety of resources including computingpower, computing platforms, storage and apps.

The idea of "computing as a service" stretches back to the 1960s, when computing bureaus allowed corporations to rent supercomputer time as opposed to purchasing one themselves. This is also how the term "cloud computing" started to be used in the early 2000s.

In the current market, the top cloud service providers include Amazone, Google, IBM, Microsoft, Saleforce etc.So there are several used for cloud computing ,including providing free access to pricey programmes and lowering the cost of setting up and maintaining machines and software because no fundation is required.

Cloud computing is increasingly common in IT systems because to its affordability, capacity, adaptability, and availability. Furthermore, crucial security elements including privacy, integrity, identification, control of access, and others have been taken into account in connection with worries about cloud security and privacy.

Every company has its own distinctive approach to cloud security, which might vary depending upon a number of factors.To create a secure and long-lasting cloud computing structure, the nation's National Institute of Standards and Technologies (NIS) has created a list of standards that can be used.

From a cloud-based server, Intruder offers vulnerability scanning for on-premises systems and cloud services.With the help this technology, cloud accounts may now be added to the standard system hardening procedure for on-site assests.

2. Literature review

The network system is more complex in lage-scale network environment.The variety of users and the openness of services and systems have centre stage, aggravating the challenge of traditional information security.

Every business has a distinct approach to cloud security, and this strategy could shift depending on a variety of scenarios.The Nationwide Institute of Standards and Innovations (NIS) of the United States has put together a set for standards that can be utilised to construct an effective and long-lasting online computing network.

Cloud security can achieved via the shared responsibility model, wherein both cloud service providers and cloud customers have their own aspects that they would need to manage and secure.

Based on previous research investigations, the proposed research survey is carried out.

We collected publications from reputable peer-reviewed article publishing sites, such as (1) IEEEXplore (2) Science direct (3) Springer link (4) Elsevier (5) ResearchGate (6) Wikipedia (7) MDPI journal.

3. Methodology

Cloud computing security consist of set of policies,control,procedures and technology that work togather for protecting cloud base system , infrastucture,Big data of cloud. Service delivery depends upon the individual cloud serviceprivider or the cloud security solutions.

3.1 Cloud Computing

Cloud computing is the way to access information and application online instead of having to build, manage, and maintain them.

Cloud security is concerned with the procedures, regulations, tools, and technologies needed to safeguard cloud computing architectures from risks and attack.Through appropriate controls and

Solution, effective cloud measures seek to keep cloud daa, applications, and services protected against both new old threats.

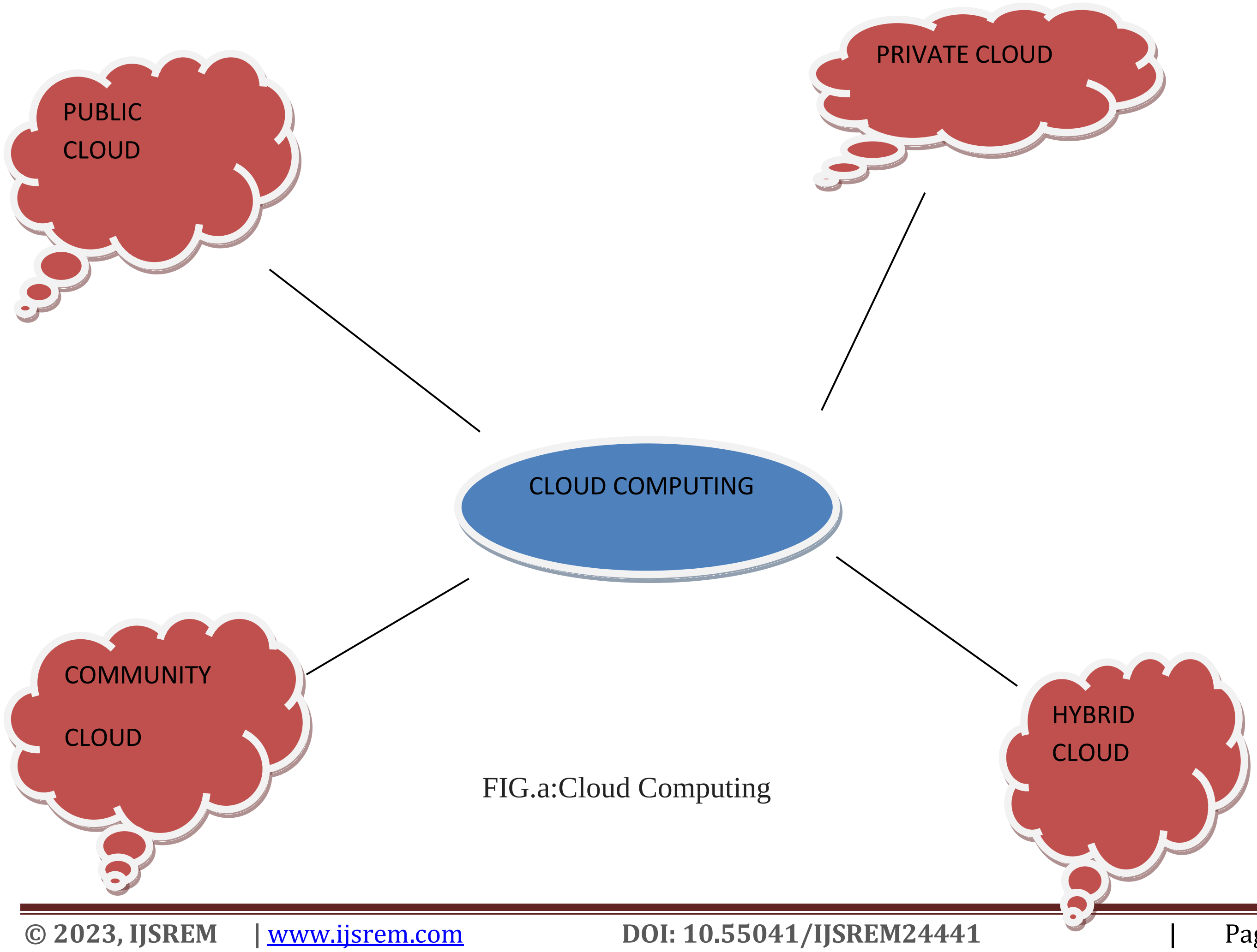


FIG.a:Cloud Computing

3.1.1 Cloud computing services

- Software as a services (SaaS)

Software as a Services (SaaS) is also known as a delivery model where the software and the data which is associated with is hosted over the cloud environment bya third party known as cloud service provider,just like your Gmail account,you use that application on someone else's system.

- Platform as a service(Paas)

It may use web-based applications to create apps that run on programming languages donated by a different organisation, including Google App Engine.

- Instrastucture as a service(IaaS)

On a subscription basis, it provides many forms of help to organisations with processing wealth, such as server, systems administration, stockpiling, and server farm their capacity.

3.1.2 Different types of cloud computing

- **Public cloud:**

Public cloud are owned and operated by third-party cloud service providers for usage by the general public.They are the exclusive owner of the cloud's infrastucture, software and hardware.The data and apps that are stored in the cloud belong to their customers.

- **Private cloud:**

Organisations in all sizes, from companies to institutions, may maintain private computers—also known as corporate clouds, internal clouds, and on-premise cloud—for their own exclusive use.When they do, they are the administrators of the cloud's foundational components and can host it locally or remotely..

- **Community cloud:**

In computing, a computing cloud is an initiative where infrastucture is shared by numerous organisations from the certain community with concern about the same thing, whether managed internally or by a third party and hosted domestically or outside.

- **Hybrid cloud:**

For the best of worlds,hybrid clouds combine private and public clouds.Organisations typically utilise public cloud to handle spikes in computing demand and private clouds for mission-critical or sensitive tasks.

3.2 Challenges/Issue in cloud computing

Security concerns in cloud computing are the main cause for concern when investing are the main cause for concern when investing in cloud services.The reason for this is that we are unable to view how the data is being processed and stored by third-party provider.

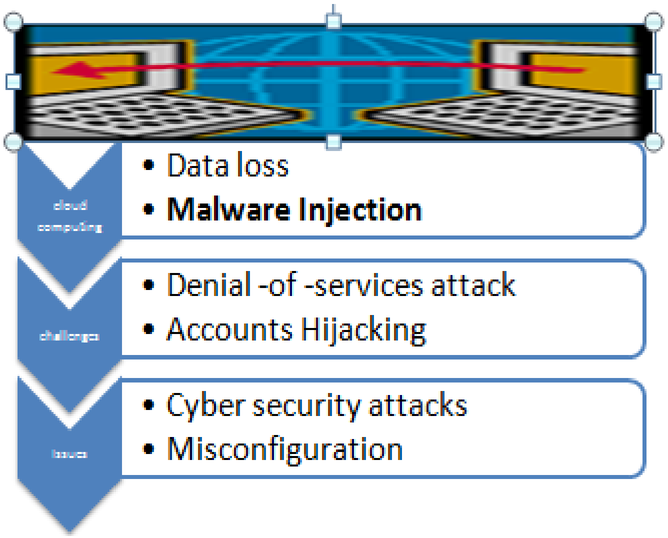


Figure (b): Challenges/Issues in cloud computing

- **Data Loss:**

Data loss is one of the drawbacks of cloud computing.A data leak is a term frequently used to describe this.Access to confidential data is available to insiders like workers and business partners.Therefor, if a cloud service's security is compromised, its probable that hackers might get our personal information or sensitive data.

- **Malware Injection**

Scirpts or pieces of code referred to as malware injections have been added to online services.It indicate that malware can be introduced into cloud services and tacken in for a part of the service or application operating on the cloud servers themselves.The possibility of installing malware is examined in the East Carolina University study examining safety issues on cloud computing vulnerabilities.

- **Hijacking of Accounts**

Hijacking of account is incresed because of increasing and adoption of the cloud in the numerous organisations which become a big issues.Using username and password or login information of yours, attackers can now remotely access sensitive data saved in the cloud and they may be change the data.

- **Denial -of -services attack**

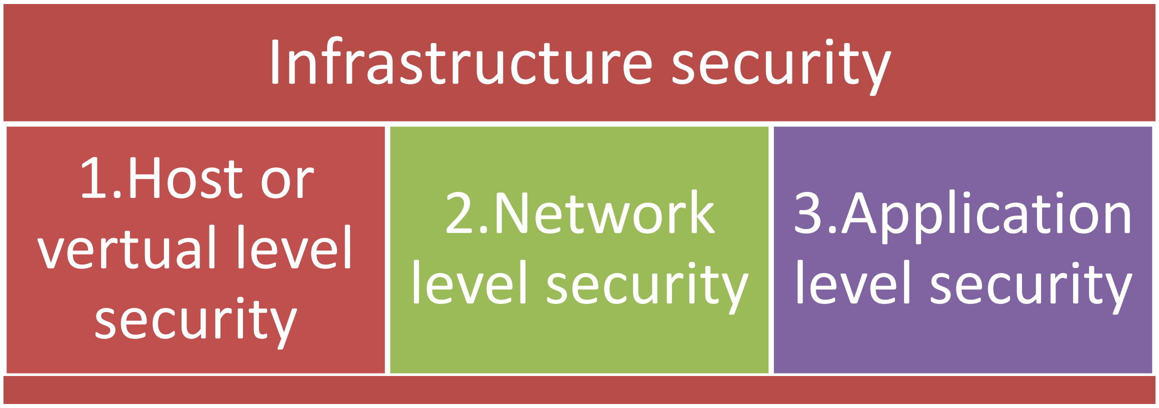
A denial-of –service (DOS) attack is designed to shut down the network or computer system to that its intended users cannot to access it. Dos attacks achieve this by offering a target with a large volume of traffic or information which results in crash.

- **Cyber security attacks**

An exploit of machines and networking is a cyber-attack.It employs malicious code to alter computer code, logic, or data and may result in online crimes including identity theft and the stealing of sensitive data.

3.3 Infrastructure security in cloud computing

Security expert mostly give important to Infrastucture security to deals with threats, risks and problems related to the protection of the information technology infrastucture of the orgaisation, including the host, network,and app levels. People are affected by threat, risk, and governance of complaince, security of the infrastructure is more closely linked to them.


Infrastructure security
1.Host or vertual level security
2.Network level security
3.Application level security

Fig(c):Infrastucture security

3.3.1 Host or Virtual level security

The security of the organization depends on the security of the device used.The host-based security sysem is automated and standardized security software used to give host oriented security in server to protect from internal and external threats.It protect multiple weak points mostly in client side. Host security can prevent from attack, minimize the impact of attack

In host security hypervertualization security is necessary.It can describe how server is set up for the preventing attack,minimizing the impact of successful attack on overall system and responding to attack when they respond.In the cloud ,rolling out a patch across the following steps:

- Update security patches on your Amazon Machine.

- Verify the results.

- Start up the virtual servers you created again.

3.3.2 Network level security

Network level security protect the networking infrastucture from misuse,distribution,modification,unauthorized access,etc.While you are uploading your data on the internet and thinking it is safe and secure ,attackers can breach data and leak confidential information or steal money.So it is necessary to secure network

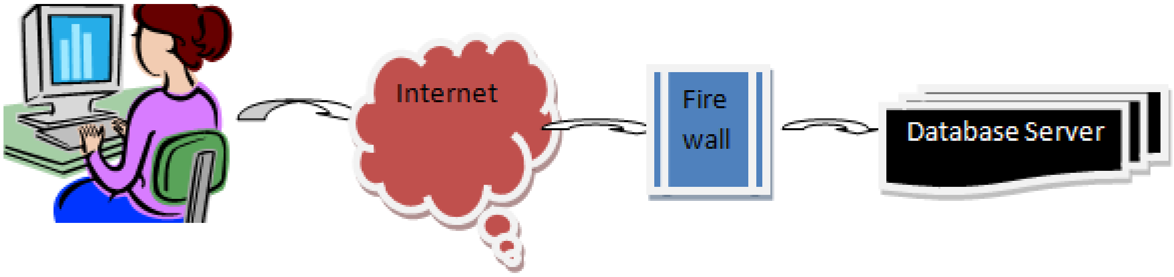
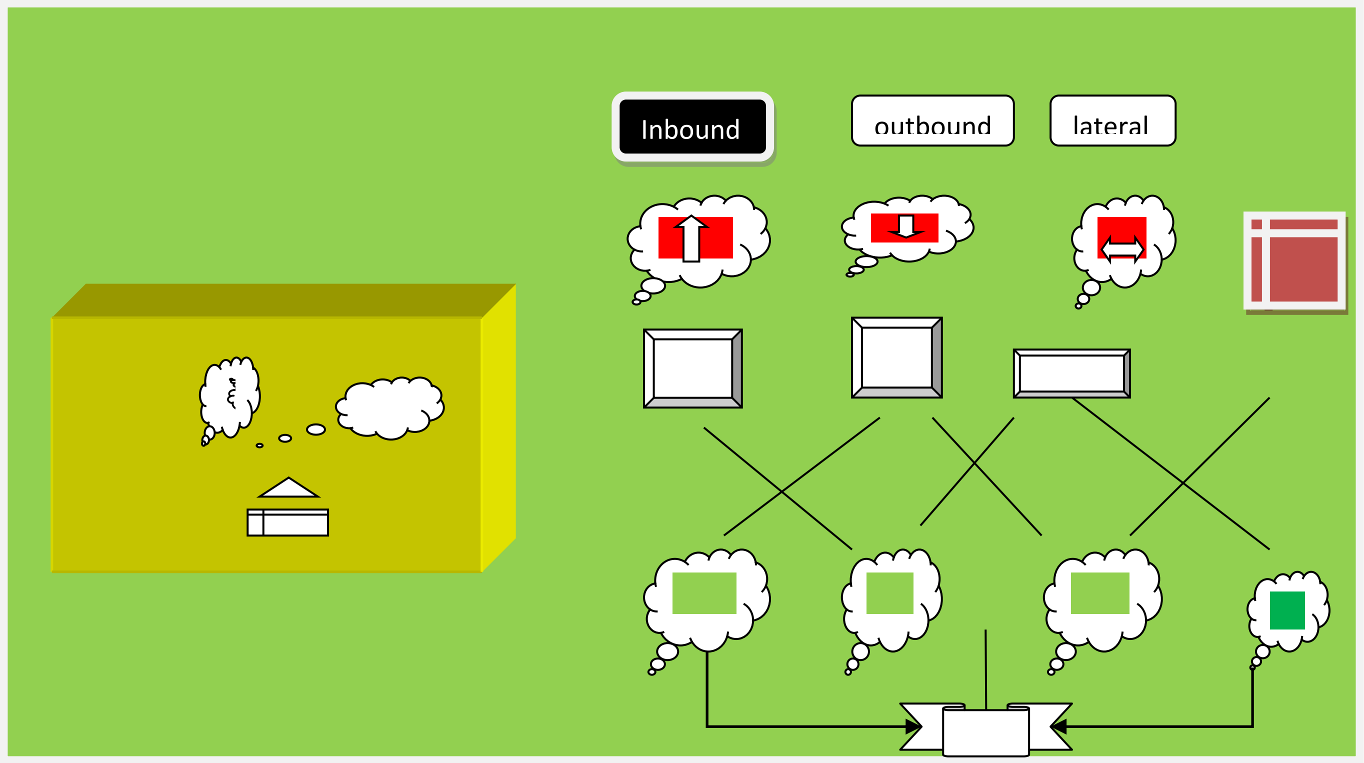


Figure (d) :Network security

The architecture of network security model is the result osf a well-through systematic process.while building the architectue,professional need to keep required in mind what type of security the organization need .There are some tool are their which help to prevent from cyber attack.The architecture may comprise element Such as control list,firewalls and other types of network secuity.



Figure(e): Cloud computing security with secure networking

Separating between public and private clouds is crucial when analysing network-level infrastructure security.If public services are chosen, changing safety standards will necessitate alterations to the network topology, thus it is essential to consider how the current network topology connects with the network topology of the provider of cloud services.

There are three levels is to used network security

- Confidential level and integrity of data transit
- Loss or no system logging /monitoring
- Availability of cloud resources.

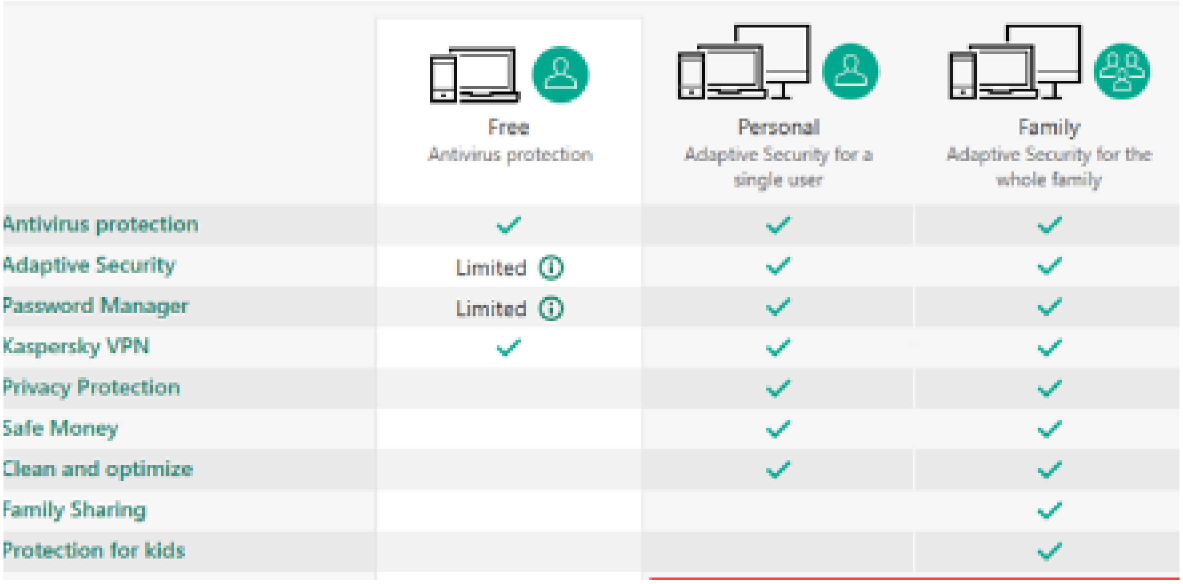
3.3.3 Application Level Security

Application safety is the process of developing, integrating, and testing safety measures within applications in order to protect them from threats like unauthorised access and alteration.

Due to their frequent access over different networks and access to the cloud, today's applications have become more susceptible to malware infections.

Opportunities and pressure to guarantee security inside every application in addition to at the network level are growing.Application security testing can reveal application-level dangers, aiding in attack response.

Examples of application safety features are authorization, authentication, encryption, logging, and application assurance.



	Free Antivirus protection	Personal Adaptive Security for a single user	Family Adaptive Security for the whole family
Antivirus protection	✓	✓	✓
Adaptive Security	Limited ⓘ	✓	✓
Password Manager	Limited ⓘ	✓	✓
Kaspersky VPN	✓	✓	✓
Privacy Protection		✓	✓
Safe Money		✓	✓
Clean and optimize		✓	✓
Family Sharing			✓
Protection for kids			✓

Figure(f):Cloud infrastucture security protection

4 Conclusion

Cloud computing solutions include on-demand utilities access, an abstraction of all computing power, and support for on-demand scale up, scale down, and scale out.There's now more explanations for stress about security.A cloud provider like Vertis, the Stavie Award winner most effective approach for safeguarding cloud-based systems with sophisticated security, whether you're moving to the cloud or are already there, can help you by making you aware of certain safety concerns. Furthermore, it has caused new security worries. You and your team may establish a multi-cloud deployment security strategy to protect your business by being aware of these top 10 cloud computing security concerns.As a result, engaging with a Stevie Award-winning vendor of cloud solutions like Veritis is the most efficient way in safeguarding the information you hold.

Reference

1. Shankar,V.,&Singh,K.(2018).Usage of attribute-driven encryption in the context of cloud computing.(Pp. 687–692) in Big Data Research.Springer,Singapore.

2. "Cryptography and Private Hassan, N. A., and Hijazi, R., "Communication."Private use of computing devices security and privacy, pp. 195–272.Apress,Berkeley,CA.

3. Alexandru, A.B., Morari, M., and Papas, G. J.-basedMPC could handle information that was encrypted.Preprint for the arXiv: 1803.09891.