International Journal of Scientific Research and Engineering Development-– Volume 5 Issue 4, July-August 2022

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Cloud Computing Design Paradigms with Security Issues

JAY PRAKASH SOJA
Assistant Professor, Department of Computer Engineering
AIT, Shakarpur, Delhi
Email: jpsoja@gmail.com

----------**********----------

Abstract:

Rapid growth of IT applications and use of IT infrastructures over the computer networks has become inevitable factor for business development and economic growth of intended organisations. Cloud refers to a network or the internet. It is a technology that uses remote servers on the internet to store, manage, and access data online rather than local drives. The data can be anything such as files, images, documents, audio, video, and more. Cloud computing is the delivery of computing services—including developing new applications and services, servers, databases, networking, hosting blogs and websites, delivery of software on demand, analysis of data, intelligence, streaming videos and audios over the internet.

Keywords: Cloud Computing; SaaS, PaaS, IaaS, DaaS, On-demand Self Service, Resource Pooling, Rapid Elasticity, Load Balancing, Multi-cloud strategy.

----------**********----------

I. INTRODUCTION

Cloud Computing is defined as storing and accessing of data and computing services over the internet. It doesn't store any data on your personal computer. It is the on-demand availability of computer services like servers, data storage, networking, databases, etc. The main purpose of cloud computing is to give access to data centers to many users. Users can also access data from a remote server. In 2002, Amazon started Amazon Web Services, providing services like storage, computation and even human intelligence. In 2009, Google Apps also started to provide cloud computing enterprise applications.

PUBLIC CLOUD

Public cloud is open to all to store and access information via the Internet using the pay-per-usage method. In public cloud, computing resources are managed and operated by the Cloud Service Provider (CSP). A public cloud is probably the most commonly understood cloud computing option. This is where all the services and supporting infrastructure are managed off-site over the Internet and shared across multiple users.The service provider provides services and infrastructure to various clients. Customers do not have any control over the location of the infrastructure. Public cloud is suited for business which require managing load. Due to the decreasing capital overheads and operational cost, the public cloud model is economical. Public cloud facilities may be available for free. Public Cloud is less secure because resources are shared publicly. Performance depends upon the high-speed internet network link to the cloud provider. The potential for cost saving is the major reason of cloud services adoption by many organizations. Cloud computing gives the freedom to use services as per the requirement and pay only for what you use. Due to cloud computing it has become possible to run IT operations as a

outsourced unit without much in-house resources. An example of a public cloud is Google.

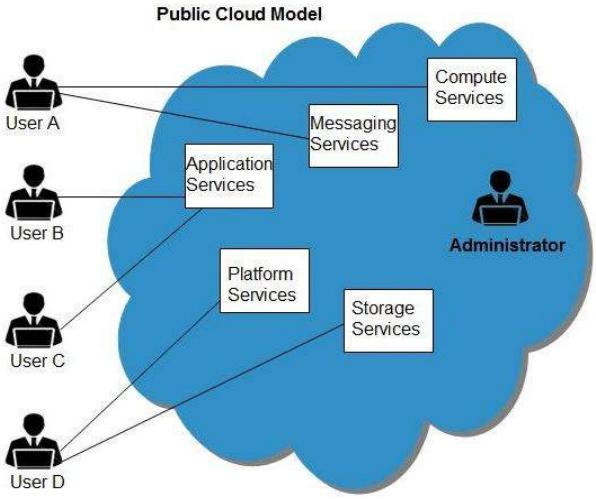

Fig-1 (Public Cloud Model)

PRIVATE CLOUD

Private cloud is also known as an internal cloud or corporate cloud**.** It is used by organizations to build and manage their own data centers internally or by the third party. It can be deployed using Opensource tools such as Openstack and Eucalyptus. A private cloud provides IT services through the Internet or a private network to select users, rather than to the general public. All the data is protected behind a firewall. Private cloud provides a high level of security and privacy to the users. Private cloud offers better performance with improved speed and space capacity. It allows the IT team to quickly allocate and deliver on-demand IT resources. The organization has full control over the cloud because it is managed by the organization itself. So, there is no need for the organization to depends on anybody. It is suitable for organizations that require a separate cloud for their personal use and data security is the first priority. An organization properly architects and implements a private cloud, it can provide most of the same benefits found in public clouds, such as user self-service and scalability, as well as the ability to provision and configure virtual machines and optimize computing resources on demand. HP Data Centers, Microsoft, Elastra-private cloud, and Ubuntu are the example of a private cloud.

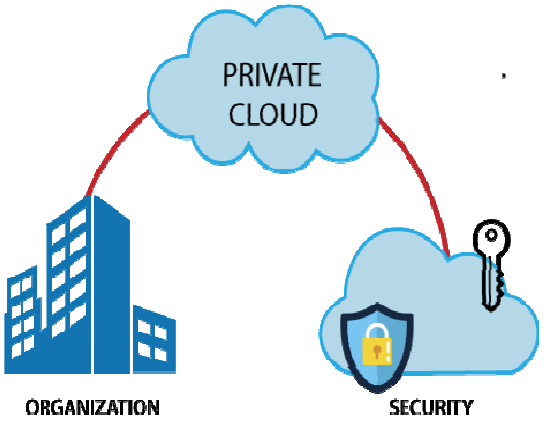

Fig-2 (Private Cloud Model)

HYBRID CLOUD

Hybrid Cloud is a combination of the public cloud and the private cloud. Hybrid Cloud = Public Cloud + Private Cloud. Hybrid cloud is partially secure because the services which are running on the public cloud can be accessed by anyone, while the services which are running on a private cloud can be accessed only by the organization's users. Hybrid clouds are capable of crossing isolation and overcoming boundaries by the provider. Therefore, it cannot be simply categorized into public, private or community cloud. It allows the user to increase the capacity as well as the capability by assimilation, aggregation and customization with another cloud package / service. Hybrid cloud is suitable for organizations that require more security than the public cloud. It helps you to deliver new products and services more quickly. Hybrid cloud provides an excellent way to reduce the risk. It offers flexible resources because of the public cloud and secure resources because of the private cloud. Google Application Suite (Gmail, Google Apps, and Google Drive), Office 365 (MS Office on the Web and One Drive), Amazon Web Services are examples of hybrid cloud.

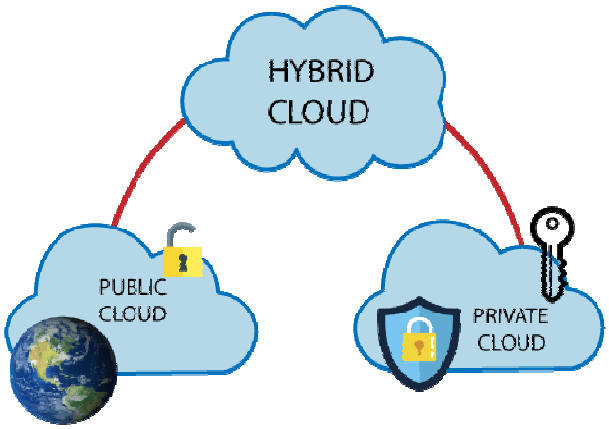

Fig-3 (Hybrid Cloud Model)

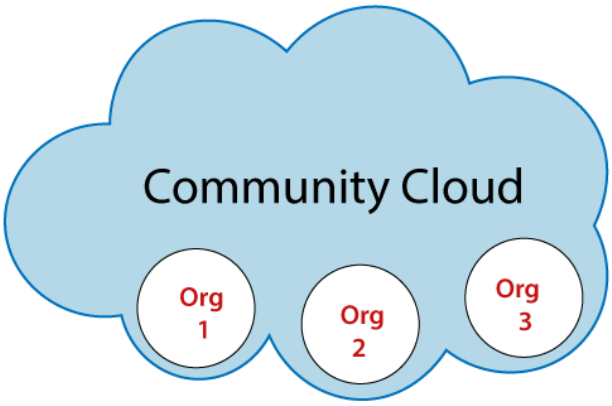

Fig-4 (Community Cloud Model)

COMMUNITY CLOUD

Community cloud allows systems and services to be accessible by a group of several organizations to share the information between the organization and a specific community. It is owned, managed, and operated by one or more organizations in the community, a third party, or a combination of them. The cost is shared by specific organizations within the community. Therefore, community cloud has cost saving capacity. It is cost-effective because the whole cloud is being shared by several organizations or communities. It is suitable for organizations that want to have a collaborative cloud with more security features than the public cloud. It provides better security than the public cloud. It provides collaborative and distributive environment. Community cloud allows us to share cloud resources, infrastructure, and other capabilities among various organizations.

CLOUD SERVICE MODELS

Infrasrtucture as a service (IaaS)

Iaas is also known as Hardware as a Service (HaaS). It is one of the layers of the cloud computing platform. It allows customers to outsource their IT infrastructures such as servers, networking, processing, storage, virtual machines, and other resources. Customers access these resources on the Internet using a pay-as-per use model. In traditional hosting services, IT infrastructure was rented out for a specific period of time, with pre-determined hardware configuration. The client paid for the configuration and time, regardless of the actual use. With the help of the IaaS, clients can dynamically scale the configuration to meet changing requirements and are billed only for the services actually used. IaaS cloud computing platform layer eliminates the need for every organization to maintain the IT infrastructure. IaaS is offered in three models: public, private, and hybrid cloud. The private cloud implies that the infrastructure resides at the customer-premise. In the case of public cloud, it is located at the cloud computing platform vendor's data center, and the hybrid cloud is a combination of the two in which the customer selects the best of both public cloud or private cloud. IaaS provides Computing as a Service (CaaS) includes virtual central processing units and virtual main memory for the Virtual machine that is provisioned to the end users. IaaS provider provides back-end storage for storing files. IaaS also works as Network as a Service (NaaS) that provides networking components such as routers, switches, and bridges for the Virtual machines. It provides load balancing capability at the infrastructure layer.

Fig-5 (IaaS-Cloud Service Model)

Software as a Service (SaaS)

SaaS is also known as "on-demand software". It is a software in which the applications are hosted by a cloud service provider. Users can access these applications with the help of internet connection and web browser. SaaS is managed from a central location hosted on a remote server accessible over the internet. Users are not responsible for hardware and software updates. Updates are applied automatically. The services are purchased on the pay-as-per-use basis. Big Commerce, Google Apps, Salesforce, Dropbox, ZenDesk, Cisco WebEx, ZenDesk, Slack, and GoToMeeting are the examples of SaaS.

Plateform as a service (PaaS)

Platform as a Service (PaaS) provides a runtime environment. It allows programmers to easily create, test, run, and deploy web applications. User can purchase these applications from a cloud service provider on a pay-as-per use basis and access them using the Internet connection. In PaaS, back end scalability is managed by the cloud service provider, so end- users do not need to worry about managing the infrastructure. PaaS provides platform (middleware, development tools, database management systems, business intelligence, and more) to support the web application life cycle. PaaS includes infrastructure (servers, storage, and networking).

Fig-6 (SaaS- Cloud Service Model)

PaaS providers provide the Programming languages, Application frameworks, Databases, and Other tools. Google App Engine is the example of PaaS.

Desktop as a Service (DaaS)

Desktop as a Service (DaaS) is a cloud computing offering where a service provider delivers virtual desktops to end users over the Internet, licensed with a per-user subscription. The provider takes care of backend management for small businesses that find creating their own virtual desktop infrastructure to be too expensive or resource-consuming. This management typically includes maintenance, back-up, updates, and data storage. Cloud service providers may also handle security and applications for the desktop, or users may manage these service aspects individually. With Desktop as a Service (DaaS), the cloud services provider hosts the infrastructure, network resources, and storage in the cloud and streams a virtual desktop to the user's device, where the user can access the desktop's data and applications through a web browser or other software. Organizations may purchase as many virtual desktops as they need through a subscription model.

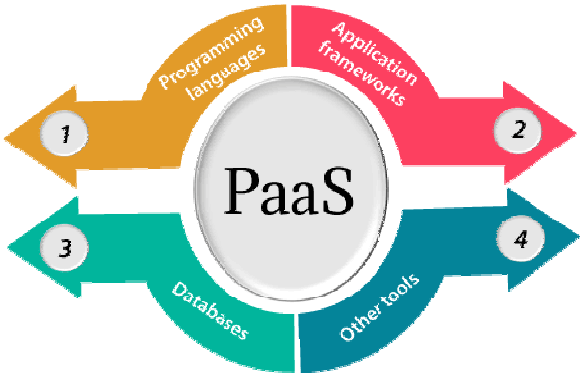

Fig-7 (PaaS- Cloud Service Model)

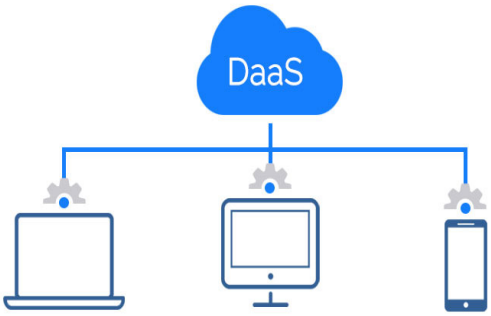

Fig-8 (DaaS- Cloud Service Model)

On-Demand Self-Service

On-demand self service allows customers to use cloud computing as required without human contact between consumers and service providers. Using the features of on-demand self-service, consumers can arrange various cloud resources as needed. In addition to being safe and attentive to the client, the self-service system must be user-friendly in order to access the various cloud resources and to track the service offerings effectively. The primary benefit of on-demand self-service generating efficiencies for both consumers and providers of cloud services

Resource Pooling

The service provider's or enterprise's computing resources are pooled to serve multiple users through a multi-tenant model (i.e., many users can access the same location's resources). These different physical and virtual resources are assigned dynamically according to demand.

Rapid Elasticity

Elasticity is a 'rename' of scalability This is the capabilities available to users can be provisioned elastically and released when no longer needed, in some cases automatically. This allows rapid scaling, up or down, according to current demand.

Load Balancing

Cloud load balancing is defined as dividing workload and computing properties in cloud computing. Load balancing is the method that allows you to have a proper balance of the amount of work being done on different pieces of device or hardware equipment. Typically the load of the devices is balanced between different servers or between the CPU and hard drives in a single cloud server. It is used to improve the speed and performance of each single device, and protect individual devices from hitting their limits by reducing their performance. It enables enterprises to manage workload demands or application demands by distributing resources among multiple computers, networks or servers.

Multi-Cloud Strategy

Multi-Cloud strategy involves the implementation of several cloud computing solutions simultaneously. It permits sharing of web, software, mobile apps, and other client-facing or internal assets across several cloud services or environments. Multi-cloud environment is used by the organisations for reduction of dependence on a single cloud service provider and improving fault tolerance.

Security Issues

Cloud service models not only provide different types of services to users but they also reveal information which adds to security issues and risks of cloud computing systems. IaaS which is located in the bottom layer, which directly provides the most powerful functionality of an entire cloud. IaaS also enables hackers to perform attacks, e.g. brute-forcing cracking, that need high computing power. Multiple virtual machines are supported by IaaS, gives an ideal platform for hackers to launch attacks that require a large number of attacking instances. Loss of data is another security risk of cloud models. Data in cloud models can be easily accessed by unauthorized internal employees, as well as external hackers. The internal employees can easily access data intentionally or accidently. External hackers may gain access to databases in such environments using hacking techniques like session hijacking and network channel eavesdropping. Virus and Trojan can be uploaded to cloud systems and can cause damage. It is important to identify the possible cloud threats in order to implement a system which has better security mechanisms to protect cloud computing environments.

Hacked interfaces and APIs

Today every cloud service and application now offers APIs. IT teams use these interfaces and APIs to manage and interact with cloud services, including those that offer cloud provisioning, management and monitoring. The security and availability of cloud services depend on the security of the API. Risk is increased with third parties who rely on APIs and build on these interfaces, as organizations may need to expose more services and credentials. APIs and Weak interfaces may expose organizations to security related issues such as confidentiality, accountability, availability APIs and interfaces are the very much exposed part of the system because they can be accessed from public networks.

Account Hijacking

Phishing, fraud, and software exploits are highly prevalent today, and cloud services add a new dimension to the threat because attackers can eavesdrop on activities, manipulate transactions, and modify data. Attackers may be able to use the cloud application to launch other attacks. Organizations must prohibit sharing of account credentials between users and services and must enable multifactor authentication schemes where available. Accounts, must be monitored so that every transaction should be traced to a human owner. The key is to protect account credentials from being stolen.

DoS attacks

DoS attacks have been around for a long time and have gained prominence again thanks to cloud computing because they often affect availability. Systems may run slow or simply time out. These DoS attacks consume large amounts of processing power, a bill the customer may ultimately have to pay. High-volume DoS attacks are very common, but organizations should also be aware of asymmetric and application-level DoS attacks, which target Web server and database vulnerabilities. Cloud providers are better poised to handle DoS attacks than their customers. The key here is to have a plan to mitigate the attack before it occurs, so administrators have access to those resources when they need them.

Flooding Attacks

In this type of attack the invader sends large number of requests for resources on the cloud rapidly so that the cloud gets flooded with the large number of requests. As per the study carried out by IBM cloud has a property to expand on the basis of amount of request. It will expand in so that it fulfills the requests of invader making the resources inaccessible for the normal users.

Conclusion

Cloud Computing is a new concept that presents quite a number of benefits for its users. But it also raises some security problems which may affect its usage. Understanding about the vulnerabilities existing in Cloud Computing will help organizations to make the shift towards using the Cloud. Since Cloud Computing leverages many technologies and it also inherits their security issues. Traditional web applications, virtualizations have been looked over but some of the solutions offered by cloud are immature or inexistent. We have presented security issues for cloud models: IaaS, PaaS, and SaaS, which differ depending on the model. As described in this paper, storage and networks are the biggest security concerns in Cloud Computing. Virtualization that allows multiple users to share a physical server is a major concerns for cloud users. Virtual networks are target for some attacks. We have focused on this distinction, where we consider important to understand these issues. Another core element of cloud computing is multi-tenancy.

References

1. Fundamentals of Cloud Computing by Pattnaik P
2. The A To Z Of Cloud Computing by Swapnil Saurav.
3. Mastering Cloud Computing by Buyya, Vecchiola and Selvi
4. Cloud Computing Simplified' by Surbhi Rastogi
5. Fundamentals of Cloud Computing by Prashant Kumar
6. Cloud Computing Black Book by KAILASH JAYASWAL and John Wiley
7. Cloud Computing by Dr Rajiv Chopra
8. Handbook of Cloud Computing by Dr. Anand Nayyar by BPB Publications

