Vivid analysis of Cloud Computing along with its security issues and challenges

Varun Ravalia, Neha Sehrawat

varunravalia@gmail.com, neha_fet@sgtuniversity.org

SGT University, Gurugram, Haryana

***Abstract:** In the modern era, technologies are being used by everyone." Cloud" refers to a collaborative expression for boundless advancements and progression. Cloud computing is a disruptive technology for providing on-demand access to data and applications from anywhere at any time in the world. Cloud computing incorporates various available innovations and technologies like virtualization, bandwidth networks, Web 2.0, browser interfaces, and time-sharing. Cloud computing enables us to share the resources like storage, applications, services, and networks without physically obtaining them. The data is stored in the databases on the servers and users/clients need to request access by sending the request to these servers. This paper includes the various details of cloud technology, its characteristics, its models alongside the challenges and problems faced in cloud computing. Here the focus is on the theoretical explanation of the cloud, models of the cloud, and the problems in the security and confrontation faced during the exertion of the cloud technology.*

***Keywords:** Cloud, Models, Security SaaS, IaaS, PaaS, Computing.*

I. INTRODUCTION

Over the last few years, advancement is done in each field. The volume of data is expanded by a huge margin along with the demand of resources required to develop and manage the facts and data. Developing and also their requirements are making it difficult to have all the resources and using them at a minimal cost. Cloud provides the stage for storing and processing data which provide features like:

1. Features:

Pooling of Assets: Asset pooling is the place where the cloud specialist organization can divide their assets between various customers, giving everybody an alternate arrangement of administrations according to their prerequisites utilizing a multi-inhabitant model.

Economical: Cloud services are economical as clients only pay administration for the space they have used. Sometimes space is allotted for free.

Broad Network Access: The clients can access data from the cloud from anywhere, they only required an internet connection and a device. This makes the cloud very easy to access and use.

2. Limitations:

Security Threat: One of the drawbacks of cloud computing is a security risk because clients are sharing their data with their service providers. Hackers can steal information from there.

Downtime: Downtime should also be considered while opting for cloud computing. Since the cloud is operated with the help of the internet and internet connection can be lost, the power supply can fail, and sometimes server maintenance is done which results in downtime.

Relies upon an internet connection**:** The Internet is the sole means to the cloud. If your connection is not working properly, the cloud service will be disconnected automatically.

II. ARCHITECTURE AND MODELS OF CLOUD COMPUTING

1. Multi-Layer Architecture of Cloud Computing

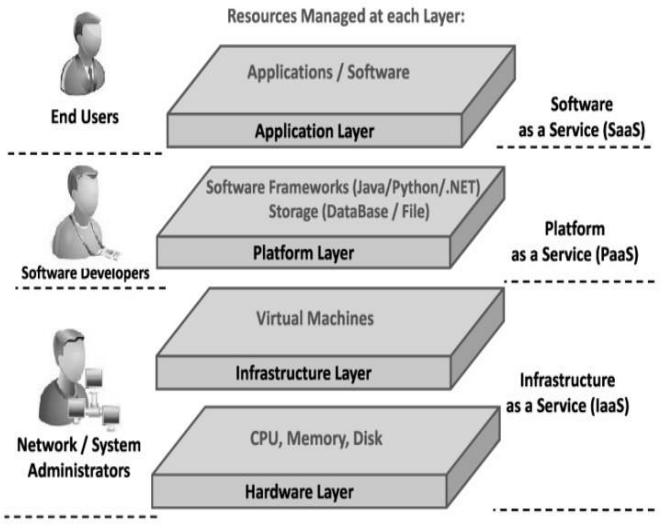
Cloud computing comprises four layers in the design: The platform layer, the infrastructure layer, the hardware layer, and the application layer. All layers are represented below:

1. The hardware layer: This layer comprises all the equipment assets needed by cloud-like actual servers, switches, power frameworks, and cooling frameworks.

2.The infrastructure layer: This layer is alluded to as the virtualization layer. It's anything but a layer that deals with a pool of computing resources. i.e. virtual pool.

3. The platform layer: The layer depends on the foundation layer; this layer comprises an operating system and application system that rearranges sending of utilizations.

4. The application layer: The application layer is the most noteworthy layer that contains the real cloud application. Cloud applications assist us with having low expenses and better execution.



2. Cloud Deployment Models

There are different kinds of cloud accessible, associations can lease the cloud as indicated by their prerequisite. Types are elaborated below:

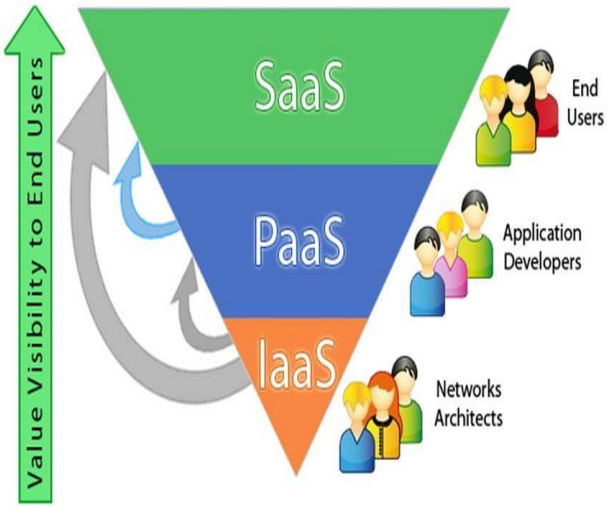
1. Public Cloud**:** This cloud is accessible to the public to use cloud services like storage, resources via the Internet. Example: IBM Smart Cloud Enterprise, Google App Engine
2. Private Cloud: This cloud is also termed the corporate or internal cloud. A private cloud is a cloud where administrations are accessible to a corporation and its individuals.
3. Hybrid Cloud: This cloud is the integration/incorporation of private cloud and public cloud.

3. Service Models

1. Software as a Service (SaaS): SaaS is additionally called cloud application administrations. Generally, these applications run straightforwardly through the internet browser implies we don't have to download and introduce these applications. Example: Dropbox, Concur.

2. Platform as a Service (PaaS): PaaS is known as cloud stage services. It's anything but somewhat like SaaS, PaaS gives a stage for software formation. Example: Windows Azure, Force.com

3. Infrastructure as a Service (IaaS): IaaS is otherwise called cloud framework services. It helps in overseeing information of utilizations, middleware, and runtime conditions. Example: Microsoft Azure, Amazon Web Services.



III. SECURITY CONCERNS AND CHALLENGES

a. Security Concerns of Cloud Computing

- One of the essential issues in the cloud is that the data is not in a physical location, alternatively, the information is put away on virtual servers.
- Access to the data is the next issue. Who has the access to it? Data is secure or not?
- The next issue for associations is the legitimacy of the cloud specialist co-op and the administration of the information.
- Recovery from the disaster is also a major concern for an organization before opting for a cloud service.
- Customers are also worried about security risks.

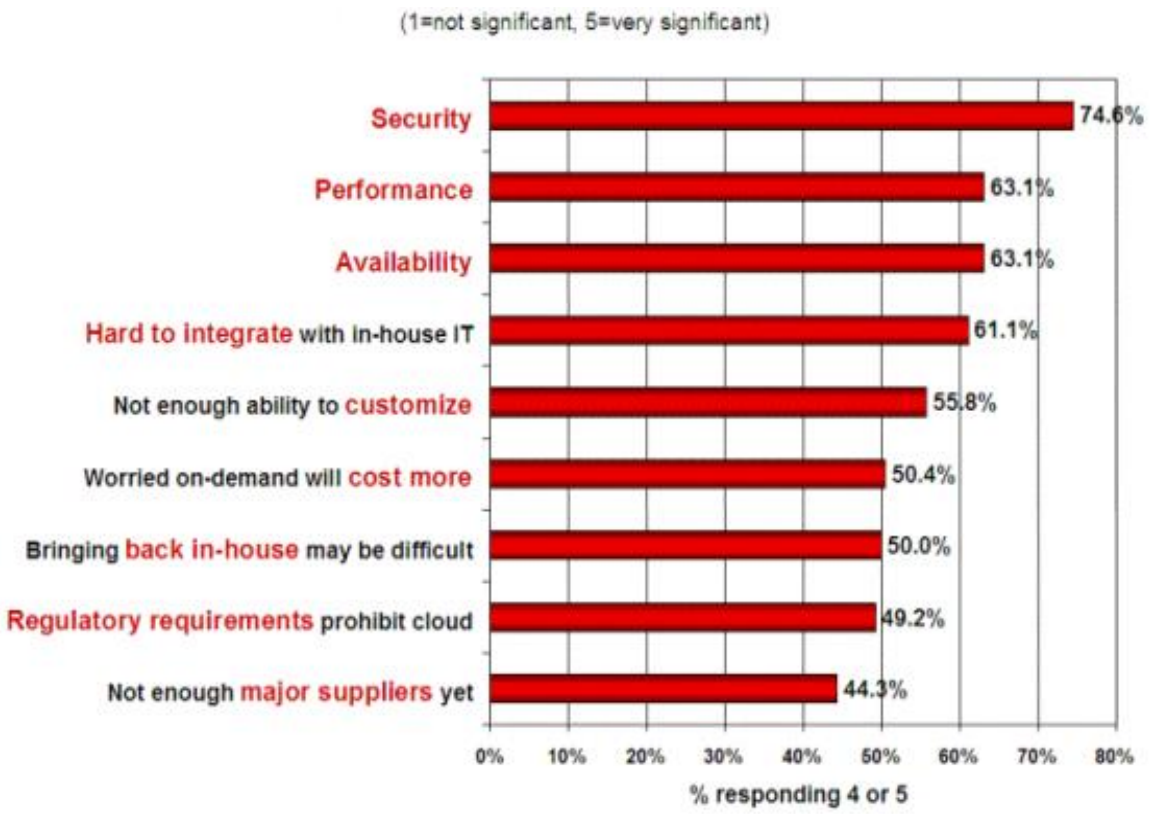
b. Solution of Challenges

- Data should be encrypted before uploading on the cloud platform. Data encryption increases the security of the data.
- Data permissions must be set so that the owner or the user can manage the authorization and grant permissions for the data.
- Data ought to be classified as heterogeneous so that there is no logical issue.
- Data backup should be done at regular intervals to ensure data protection and data backup consist of all the data without any change.
- Data consistency should be maintained at every interval and user information must be protected and data recovery options should be available.

c. Security attacks and their mitigation

S.no	Attacks	Explanation	Mitigation
1.	Virtualization Attack	This is done by rootkit in hypervisor or VM escape. In this attacker can get access to the VM machine and the host OS.	(Instruction Detection System) IDS and (Instruction prevention System) IPS helps in avoiding VM attacks.
2.	Zombie Attack	Requests to access the network are flooded by the user which is known as Zombie Attack. Due to this Denial of Service (DOS) occur.	Control is done by Authentication and Authorization of IPS and IDS.
3.	Service Injection Attack	In this attack, an attacker attempt to inject malicious services by choking the functionality of cloud services.	By the Strong segregation between the VMs Service integer checking module
4.	Metadata Spoofing Attack	Here, attackers amend the WSDL file at the time of delivery.	Mitigated by the strong invocation code flow of WSDL.
5.	Phishing Attack	Attackers can change the link of the website and redirect the users to a false or fake website and steal their information.	It is controlled by better implementation of authentication protocol.
6.	Backdoor Channel Attack	This attack is passive and to access the data of people remotely.	By authentication and isolation between virtual machines.
7.	Malware Injection Attack	This attack includes execution, broken authentication scripting by malicious files.	Good encryption and authentication of data.
8.	Wrapping Attack	This attack includes translating SOAP messages between web servers and users.	By the security validation of the SOAP message mechanism.

d. Significance of Security in Cloud Computing



The factual diagram given above addresses the result of the review which was controlled by the IDC (International Data Corporation) in August 2008 amid the expert business and IT heads about the issues and loopholes which influence the working of Cloud Computing and Cloud administrations.

The study results show that security is the most extreme need of individuals and associations.

Another overview shows that 86% of the senior business heads are a lot of inspired by Cloud Computing and over 90% of these individuals are stressed over the protection and security of information in the Cloud.

From this overview, we come to realize that security is a significant issue among every one of the determinations that influence the presentation, working, and progression of Cloud Computing.

IV. CONCLUSION

Cloud computing is a technological development that has a massive impact on the world. Cloud technology has evolved a lot in recent years. Cloud Computing services include data storage and processing to the software usage. It has enormous benefits however there is a lot of exploration still needed in it. Cloud computing is used by users and organizations by multiple cloud service providers. After all this, there are still protection and security issues. These security issues should have been contemplated and settled. New security techniques need to be developed for better isolation of the user's data. Cloud computing also provides various benefits like low cost, resource sharing, broad access, and mobility. This technology makes life easier for people around the globe. It makes use of the internet and provides resources to the clients who needed them. The cloud providers must provide security and maintain the integrity of the data which is present on the cloud. It should provide availability of resources for the users and also deliver the data precisely and maintain the confidentiality of the data. In the coming years, there will be better authentication, encryption, and validation of client information. This paper has highlighted the description of the cloud and the security concerns. As the development will be done in the coming years, cloud computing will be more useful with the least number of issues and challenges.

REFERENCES

i. Nazia Majadi, "Cloud Computing: Security Issues and Challenges" International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July 2013.

ii. Grobauer B., Walloschek T. and Stöcker E., "Understand-ing Cloud Computing Vulnerabilities," IEEE Security and Privacy, vol. 99, 2010.

iii. R. Velumadhava Rao, K. Selvamani, "Data Security Challenges and Its Solutions in Cloud Computing", ICCC2015.

iv. Cloud Computing Bible, 2011, Wiley Publishing, Inc., Indianapolis, Indiana, pg. 8-9.

v. Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing", Recommendations of the National Institute of Standards and Technology, September 2011, Special Publication 800-145.

vi. Garima Gupta P R Laxmi, Shubhanjali Sharma, "Survey on Cloud Security Issues and Techniques"2011.

vii. S. Vashisht, S. Jain, and R. S. Mann, "Software defined uav-based location aware deployment scheme for optimal wireless coverage," in2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech). IEEE, 2019, pp.907–912.