# A Survey on Cloud Computing Model Configuration Security Issues with Proposed Solutions

**Bhawna Talwar**

*Assistant Professor, CT Institute of Higher Studies, Shahpur, Jalandhar*
*bhawnatalwar2@gmail.com*

**Anuj Kumar Gupta**

*Professor, Chandigarh Engineering College, Mohali, Punjab, India*
*anuj21@hotmail.com*

## Abstract

*Cloud computing provides vast connections of remote servers and networks on the internet which allow users with the option to store the information and documents on a virtual storage base. The cloud computing speed characteristic, security issues and impacts have been a popular subject among the users. Cloud computing allows to store, manage and process data on the cloud which makes storage option easier. This research helps to get overview of cloud computing configuration management models which includes its service and deployment models. Also this paper examines the development in cloud computing with its major security threats and dangers. At the last, a solution has been proposed to improve the management models structure of cloud computing.*

***Keywords***—*CSP, IaaS, SaaS, PaaS.*

## 1. INTRODUCTION

Cloud refers as the services over internet, which provides certain physical storage base. Computing is the hardware devices and remote servers which act as the path for accessing the cloud. Figure 1 represents the interconnection of cloud servers and cloud remotes upon physical hardware components that are used to access cloud storage.

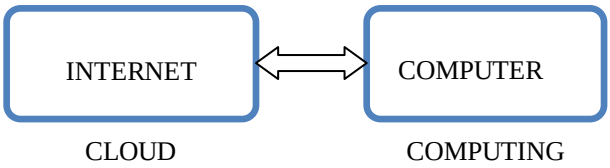


Fig 1. Cloud Computing

Therefore, cloud computing can be defined as the model which provides the user with different computer resources such as networks, servers, storage, applications and services [1].

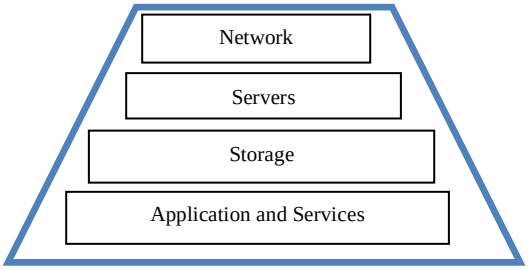


Fig 2. Pyramid Model of Cloud Resources



ISSN: 2456-1118

In figure 2 the representation of cloud resources which cloud remote servers provide to the users is shown in pyramid structure.

## 2. WHY CLOUD COMPUTING IS REQUIRED?

In past, user run applications or software programs which were first downloaded on a physical computers which creates the issue of computer memory space requirements in bulk. Since cloud computing allows users to access the same kind of applications on the internet itself without downloading it and thus cloud computing has proved to be more beneficial to save memory space in user's computer. In previous approaches storing programs and applications on physical storage areas have the another major drawback that is the data was not fully secured as if the hard drive could crash and thus the chances of getting back the original data on the user computer becomes difficult. Hence recovery of data was difficult which now cloud computing has made it easier. So, storing, processing, and managing of data is easier and recovery can be done easily by using cloud servers provided by cloud computing vendors.

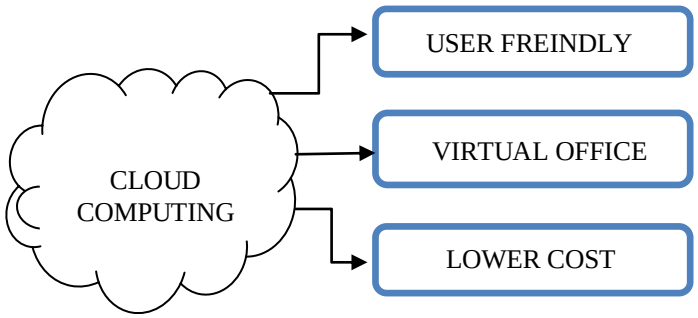


Fig 3. Requirements of cloud computing

In figure 3, it is shown how cloud computing is becoming a basic need for the users. The following factors which creates need for cloud computing have been described below:

- **User Friendly**: Cloud technology is simple and easy to use as it reduces the complexities of information technology. Cloud users are not needed to have extensive technological skills to run and configure complex systems as infrastructure on the cloud is provided by Cloud service providers to develop the applications. Cloud computing provides vast options of storing data and information on the internet and can be retrieved anywhere within no time.

- **Virtual Office**: As long as employee has internet access, they can work from anywhere called virtual office facility of cloud computing. It helps in productivity and work life balance of an employee. Employees are not tied up from the load to be present each day in offices. They can access their office data from cloud storage. The process of virtual office is helping to grow the productivity of corporate sectors. Cloud computing is helpful and will be a better prospective for companies and organizations prosperities.

- **Lower Cost**: It is helpful in business productivity as there is less capital expenditure. The excessive use of equipments and infrastructure which are provided by cloud vendors has make the creation of applications cheaper. Cloud computing provides users with the option to store extensive workloads on cloud servers which has proved the most beneficial option for corporate sectors as it is reducing issues of cost of managing business applications and storing massive business data. So, Storage and processing of data is a lot easier nowadays by using cloud.



ISSN: 2456-1118

## 3. PROS & CONS OF CLOUD COMPUTING

### *3.1Pros of Cloud Computing*

- **Anywhere Access:** The advantage in cloud computing is that a user's data is not physically on its computer. If it is stolen or lost, or any how hard disk breaks down, the user can start working again immediately on another computer using cloud where the data is stored.
- **Storage Space:** Cloud provides vast storage capacity to the users for storing of data and information or private documents. So, running out of storage space on user's computer is now no longer to be concerned by the user because cloud computing provides cloud servers. These cloud servers provides the virtual storage components which helps the user to save their massive data online and thus can be retrieve at any time.
- **Backup and Recovery**: A cloud service provider (CSP) handles the recovery of information making retrieving of lost data easier and faster. CSP stores user's sensitive data which if vanished on user's computer due to hardware failure or by user negligence can be recovered later by using cloud servers as these servers have backup for these sensitive data on data servers. It has used RAID technology for storing data in redundant to overcome the data recovery problem.

### *3.2 Cons of Cloud Computing*

- **High Speed Internet Availibility:** For accessing and managing heavy workloads on cloud drives , high speed or well established internet connection is required. If there is a connection of lower speed intenet then it would a lot harder to access the data stored on the user's drive . So,to ease the workloads of data stored on cloud users need to have a high speed internet connection.
- **Security Dependancy**: Data security on cloud depends on certain user as well as on cloud server provider. So the security is main concern in cloud computing because there are many threats and bugs which can cause harm to the stored information and documents of the users. Various security issues fixes are not even applicable and it affects in the form of spams, opening links containg virus, destroyed significant files and many more. Thus cloud computing can not said to be fully secured.
- **Control and Reliability**: "Google drive" a cloud service provided by the gmail even incured with security threats. Security issues regarding cloud reliabilty arose when some hackers attacked google drive on gmail with a spam email called as snooping. Snooping raisd questions in the mind of cloud users against the reliability and control of the IT pros on cloud servers .

## 4. SERVICE MODELS OF CLOUD COMPUTING

Cloud computing providers offer the services according to several fundamental models. The most common cloud computing service models are Software as a Service, Platform as a Service and Infrastructure as a Service model in figure 4.



ISSN: 2456-1118

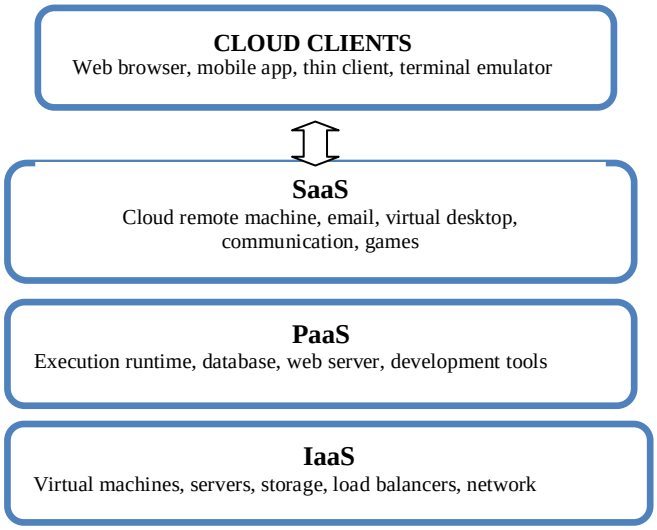


Fig 4. Service Model of Cloud Computing

- **Software as service (SaaS):** It is also known as "on-demand software" which carries the capability to provide the user to access to application software and databases. The user does not control or organize the cloud infrastructure which includes network, servers, operating systems storage, and individual application capabilities, but with the possible exception of limited user specific application configuration settings [6].
- **Platform as a service (PaaS):** In PaaS application developers can develop and run the software on a cloud platform without concerning issue of the cost and complexity of buying and managing the hardware and software layers [6]. PaaS offers platform to build applications such as Microsoft Azure and Google App Engine, also the computer and storage resources which scale automatically to match application demand so that the cloud user does not have to allocate resources manually.
- **Infrastructure as a service (IaaS):** The capability provided to the business users is processing data, storage, networks, and other fundamental computing resources where the business users will be able to deploy and run arbitrary software, which can include operating systems and applications. The users does not manage or control the cloud physical infrastructure but has control over operating systems, storage, deployed applications, and possibly have limited control of select networking components [6].

## 5. DEPLOMENT MODELS OF CLOUD COMPUTING

A cloud deployment model represents a specific type of cloud environment, mainly famed by ownership, size, and access. There are four common cloud deployment models [5] represented in figure 5 and are described below.

- **Private cloud:** The cloud infrastructure is operated solely for an organization. It may be managed by the organization or by a third party.
- **Community cloud:** When the cloud infrastructure is shared by several organizations forms a cloud community model. It supports a specific community that has shared concerns such as organizations mission and policy, security requirements and compliance considerations. It may be managed by the organizations itself or by a third party.
- **Public cloud:** The public cloud infrastructure is made available to the general public or business users. It is owned by an organization selling cloud services.
- **Hybrid cloud:** The cloud infrastructure is a composition of two or more clouds (private, community, or public) which remains unique entities and are bound together by standardized



ISSN: 2456-1118

technology that enables data and application portability (e.g., cloud replete for load balancing between clouds).

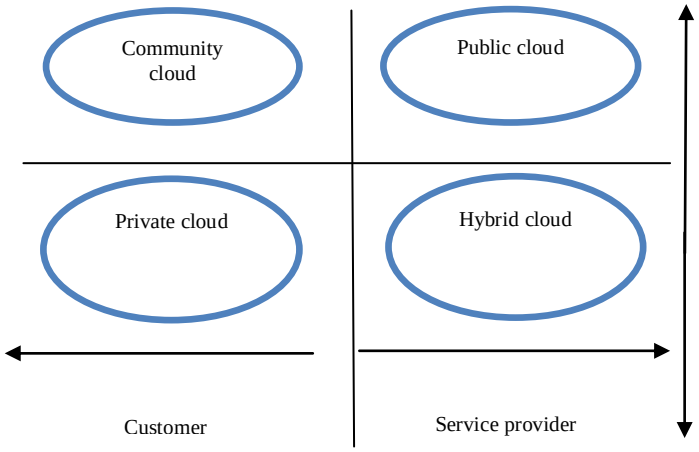


Fig 5. Representation of Deployment Model of Cloud Computing

## 6. Service Models Issues Related to Cloud Computing

Cloud Computing has features of flexibility, cost-effective, and proved as a delivery platform for providing business or consumer information technology services over the Internet [3]. However, service models of cloud computing are mainly considering the outer vulnerabilities, threats, risks and suitable requirements but solutions of security threats for cloud computing is hardly showing any results. The improvements needed to be concerned are secure Cloud systems, Cloud security, delivery models security, SaaS security, Paas security, IaaS security.

## 7. Deployment Models Issues Related to Cloud Computing

Networking, platform, storage, and software infrastructure are provided as services in the cloud deployment model that scale up or down depending on the demand [4]. The three main deployment models in the cloud computing model are as follows:

- **Private cloud:** Private cloud is used to imitate cloud computing on private networks. It is configured within an organization's internal enterprise datacenter. In the private cloud, virtual applications provided by the cloud server provider and scalable resources are pooled together. Then these are available for private cloud users to share and use.

- **Public cloud:** In the public cloud the cloud resources and applications are managed by the organization itself. Public cloud describes cloud computing in the established conventional resources which are provisioned on a self-service basis over the Internet, using web applications or web services, from third party service provider who shares resources which results in hacking of shared data saved on these resources. Public clouds are less secure than the other cloud models. It is so because it places an additional burden of ensuring all applications and data accessed on the public cloud on the users which are subjected to malicious attacks.

- **Hybrid cloud:** It provides virtual information technology solutions through a mix of both public and private clouds. Hybrid cloud has feature of private cloud which is centrally managed, and constrained by a secure network. Hybrid Cloud when contains public cloud features then it provides less secure control of the data and applications and allows various parties to access information over the Internet. This cloud has an open architecture that allows interfaces with other management systems and thus malicious attacks can easily penetrate in its architecture and change



ISSN: 2456-1118

the configuration settings of business user software's build on this cloud architecture. This model uses configuration which combines virtual and physical architecture of user and cloud service providers, which lacks in security of virtual server and network resources used by users.

## 8. SECURITY DANGERS TO CLOUD COMPUTING

The principal security dangers to cloud computing include dangers that currently exist in pre-cloud computing. Cloud computing heightens the risks in certain dangers, such as data corruption, while introducing some new risks, such as virtualization and multi-tenancy [7, 8].

- ***Virtualization and multi-tenancy***
  Cloud offers take advantage of economies of scale, offering shared services within their infrastructure. Virtualization and multi-tenancy architectures make this possible.
- ***Nonstandard and vulnerable APIs***
  Application programming interfaces (API) are the software interfaces that cloud providers offer to allow their customers access into the services. Cloud API is not standardized, forcing users of multiple cloud providers to maintain multiprogramming interfaces, increasing complexity and security risk.
- ***Internal security breaches***
  The IT industry has well documented that over 70% of security violations are internal – This threat is amplified in cloud computing as both IT providers and consumers are under a single management domain.
- ***Data corruption or loss***
  Data corruption or loss is amplified since the cloud provider is the source for a company's data, not the company itself. These operational characteristics of the cloud environment, at the PaaS and SaaS layers, amplify the threat of data loss or leakage increase.
- ***User account and service hijacking***
  User account and service hijacking occurs when a attacker obtains your cloud services information and uses it to take over your cloud access. If attackers gain access to a cloud user's identification, they can snoop on activities and transactions, manipulate or steal data, return falsified data, and redirect clients to illegal sites.

## 9. PROPOSED SOLUTIONS TO THE THREATS IN CLOUD COMPUTING MODEL

- Network Security can be ensure by using strong passwords and encryption/decryption techniques on sensitive data transfer.
- Application with Interface Security can be done only if code deployed by users is tested by using sandbox testing.
- Server Security can be enhanced by using intrusion detection system [2] and firewalls to prevent from malicious attacks.
- Data Security using data masking techniques and security questions on deleting sensitive data should be considered to avoid loss of sensitive data.
- The private cloud can be considered as much more secure model than that of the public cloud because of its limited access to the external exposure. Hence the preference should be given to private cloud over public cloud when there is a requirement of securing the sensitive data of organization.

## 10. CONCLUSION

There are number of security beaches and spam which are harmful for a user private documents and files. Since, advanced information technology techniques are trying and achieving most of it for making security protocols for the cloud drives and applications which would make more users to fully use and support cloud computing in the future. Thus this research enlightened the major issues in cloud computing with the proposed solutions if applied on these issues can make cloud



ISSN: 2456-1118

computing configuration model to be the most popular secured technology model which provides services anywhere without worrying for security of data.

## REFERENCES

[1]. Ahmed S, Raja M. (2010) 'Tackling Cloud security issues and forensics model', High Capacity Optical Networks and Enabling technologies (HONET), 19-21 Dec, pp. 190-195.
[2]. Jun-Ho Lee, Min-Woo Park. (2011) 'Multi level Intrusion Detection System and Log management in Cloud Computing', Advanced Communication Technology (ICACT), 13th International Conference 2011, 552-555.
[3]. Kandukuri B.R, Paturi V.R. (2009) 'Cloud Security Issues', International Conference on Services Computing, 21-25.
[4]. L. Savu. (May.2011) 'Cloud Computing: Deployment Models, Delivery Models, Risks and Research Challenges', International Conference on Computer and Management, 1-4.
[5]. Mukharjee K, S.G. (2010) 'A secure Cloud Computing ', 2010 International Conference on Recent Trends in Information Telecommunication and Computing, 369-371.
[6]. Mathisen, Eystein. (2011) 'Security challenges and solutions in Cloud Computing', Digital Ecosystems and Technologies Conference (DEST), 5th IEEE International Conference, 208-212.
[7]. Pearson, S. and Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. Cloud Computing Technology and Science, 2010 IEEE Second International Conference, 693-702.
[8]. Anuj Kumar Gupta. (2015) "Cloud Computing: Concepts and Challenges", Asian Journal of Computer Science and Technology, ISSN: 2249-0701, 4(2): 27-30.

## Authors

Bhawna Talwar is working as Assistant Professor in Computer Applications Department affiliated with GNDU (Guru Nanak Dev University), Amritsar in CT Group of Institutions since June 2013.

Anuj Kumar Gupta is working as Professor in Chandigarh Group of Colleges. He has a teaching experience of 15 years. He has completed his PhD in Mobile Ad hoc Networks and his area of expertise is Wireless Networks. He has guided many M.Tech. research scholars and is also guiding Ph.D. scholars.



ISSN: 2456-1118