# Security Issues In Cloud Computing

**V Raviteja Kanakala, K.Chandra Shekhar, G.Vijay Kumar**

**Department of Computer Science & Engineering**

**Pragati Engineering College, East Godavari, Andhra Pradesh, India.**

***Abstract***

*The world is now experiencing internet based computing. Cloud computing is one of the types of internet based computing. Cloud computing is an evolving technology through which users can get anything as service from software to high end infrastructure including datacenters through online on-demand. Cloud computing was added to IT Jargon in early 2007 but till now many big IT companies don't trust cloud computing completely because of some concerns about security, regulation, compliance, and performance. Cloud computing security is as much process as it is trust. This paper discusses about different complications occurring in cloud computing in the area of security.*

*Keywords: Cloud computing, datacenters, Cloud computing security.*

## I. Introduction

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [2]. Most of the organizations are changing their path to cloud computing from the traditional way of computing. Cloud computing, often referred to as simply "the cloud," is the delivery of on-demand computing resources everything from applications to datacenters over the internet on a pay-for-use basis [3]. In cloud computing everything is provided as a service but not as a product which leads to a trend to lease an IT product to get the benefits of it instead of buying, establishing and managing that product. The collective working of virtualization and networking is cloud computing. Cloud computing technology emerged basing on the ideas of several other computing research areas like High Performance Computing, Grid computing, Virtualization, parallel computing, Cluster computing which are the child technologies of distributed computing. Distributed computing which is the base technology from which cloud computing was emerged had several issues like scalability, internet delay and security. Most of these problems were solved by Cloud computing but security remained as major obstacle. Security is one of the main reasons because of which big companies are not trusting cloud completely. The cloud paradigm contains some essential characteristics like ubiquity, convenient and on-demand network access through which a consumer is able to manage all the computing capabilities without the requirement of human interaction with each service provider. A Broad network access needed because all the functionalities will be running over the network. The meaning of on-demand self service is to create resources and also allowing to resize the resources based on the workflow models. The cloud model is composed of some service and deployment models.

## II. Service Models of Cloud Computing

- **Software as a Service (SaaS)**: Software as a Service means providing the software to the user as a rental service. Buying some of the software costs high, in such cases we can go for the pay-per-use option, which reduces the cost for the end-user. Software as a service is the fisrt implemented cloud service.
- **Platform as a Service (PaaS)**: Platform as a service means providing a computing application interface to the client as a service to develop applications as per their requirements. This service aims to provide the capacity to the customer to deploy the cloud infrastructure using the programming languages, tools and other commercial components.
- **Infrastructure as a Service (IaaS)**: In this service the client can get control over some of the underlying infrastructure of cloud such as networking, processing, storage, and other fundamental resources. The better option is to avail the outsourced resources by stable outsourcing organizations.

## III. Deployment models of cloud computing

Deploying cloud services to clients by various cloud vendors are generally classified into following types with derived variations that deal with specific requirements as follows

- **Public Cloud**: In Public cloud resources are deployed to the end user through internet via web applications of the cloud vendor which owns the cloud. The public cloud is available to the general public for open use. Other than the advantages of public cloud deployment model there are some security and quality risks in this deployment model.
- **Private Cloud**: In this deployment model the cloud resources are maintained by single private organization only. Since the deployment is done in the organizations own datacenter separately without any interference of other organization data the security level in this type of deployment model will be high.
- **Hybrid Cloud**: This deployment model will have the combined properties of both public and private cloud models. In this hybrid model the infrastructure management for private enterprises will be done by several internal and external service providers. hybrid cloud is an environment that employs both private and public cloud services.

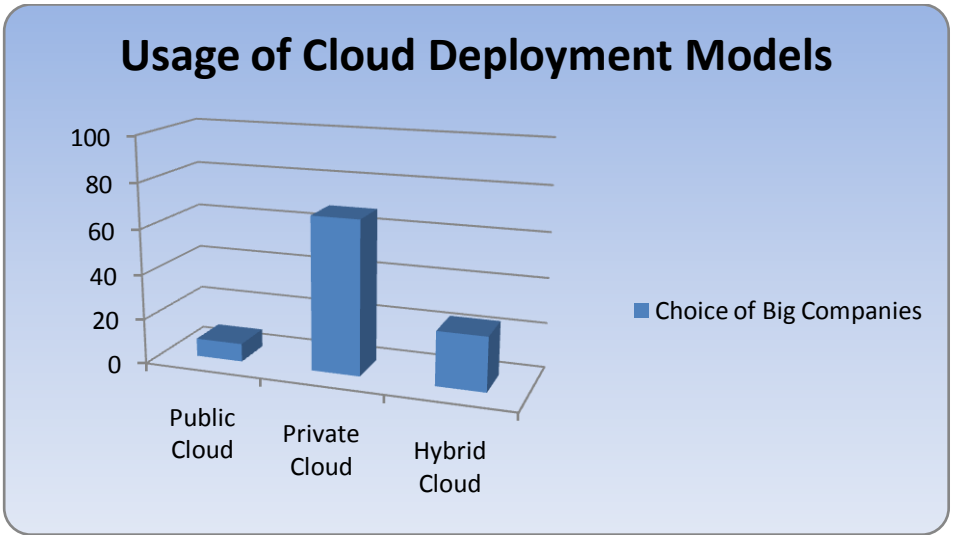



**Figure.1 Survey on choice of big companies among different Cloud Deployment models**

In Today's world Companies are realizing that they need many different types of cloud services in order to meet a variety of customer needs. Most small and medium sized companies like the idea of Cloud Computing. But most big companies opt for private cloud or the hybrid cloud and they oppose public cloud for security reasons [5].

## IV. Issues in Cloud computing

Despite the benefits there were many issues in cloud computing to be solved. Customers must understand these issues before adopting cloud computing. The following are the major issues cloud is facing today.

- **Technical Issues**:

In cloud computing frequent occurrence of risks are in the technical area of cloud computing. Even though there is quick progress in the advancement of cloud technology still there are some problems which are causing serious obstacles to the companies adopting cloud computing.

- **Legal Issues:**

As the concept of cloud computing technology is different from the traditional IT there are some changes in the legal and judicial areas

- **Performance Issues:**

The potential of a technology can be calculated by its performance only. Despite the various advantages in cloud technology the performance factor is not stable. Applications which are performing well in datacenters may not perform the same in the cloud [18]. The cloud providers should test their performance levels on their by conducting tests like network speed at different geographical areas, Application flexibility on different platforms etc [19].

- **Security Issues in Cloud Computing**

The major concern of many big companies for adopting cloud computing is security. Generally in the cloud, security will be completely under the control of service provider; this is the reason why the client feels insecure about his data. This service model provides security as a service platform which makes the client feel more secure with his own private security keys. This service should be offered by the cloud provider itself in order to make the clients feel more secure and to increase the number of users in the cloud environment. Among the several issues in cloud computing technology the major issue was security. Many organizations which adopt cloud computing will store their data which is confidential but they don't have any control over it. As per the reports of the experiences of customers there are attacks on the data such as cloud-based botnets for example DDOS (distributed denial of service attack). Trust of the customer is very important for a technology like cloud which can be gained by improving the security.

## V. Security concerns in cloud computing

Among all the issues being faced in cloud technology security issue is the major one. Security is a very broad area and we cannot deal all the issues as a whole. So, in this paper several categories of security issues that might arise in different sub-areas of cloud security were analyzed.

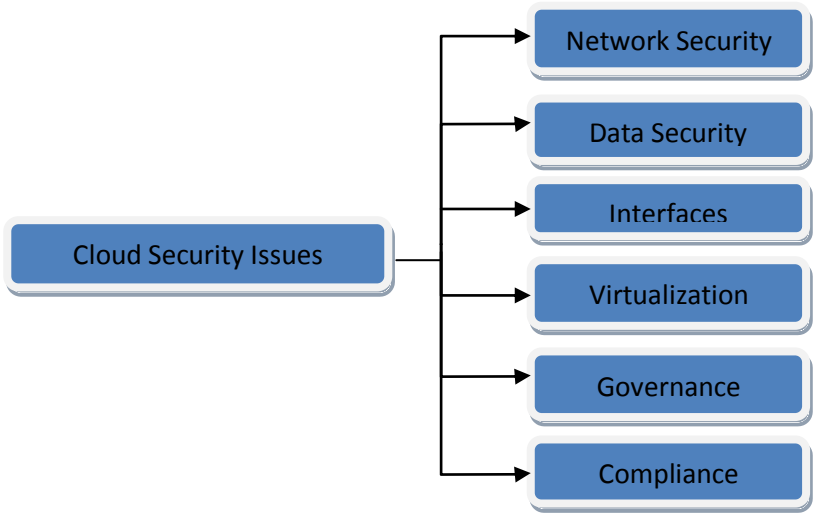
- **Network Security**

Network security is one of the major areas where problems may arise while network communications were being happened and while configuring the cloud infrastructure.

**a)** ***Transfer Security:*** One of the major areas where problems arise due to security attacks like sniffing, spoofing, etc is Transfer Security. We can control the security attacks by using VPN (Virtual Private Network) mechanism.

**b)** ***Firewalling:*** Firewalls plays major role in preventing attacks of Insiders & Outsiders, Denial of Service attack, etc. By using firewalls efficiently we can stop all the attacks from outside the system.

**c)** ***Security Configuration:*** The level of security and privacy depends upon the configuration of protocols and systems.




- **Interface Security**

Security attacks were also possible with vulnerable User Interfaces, Administrative Interfaces & different Programming Interfaces.

a) ***Application Programming Interface:*** Security for API will prevent malicious attacks on the programming interfaces using which we will access virtualized resources.

b) ***Administrative Interface:*** Administrative Interface deals with controlling resources in IaaS, PaaS, SaaS from a remote place. If Administrative control is vulnerable to attacks then the total cloud system will be in risk.

c) ***User Interface:*** Security for user interface implies the need of adapting security measures for exploring the resources and tools.

d) ***Authentication:*** Secured Authentication mechanisms are needed for preventing plethora attacks which occur commonly in resource sharing environment.

- **Data Security**

Many big companies were not adopting cloud computing technology even though they are interested because they don't want to store data in resources which are in the control of cloud vendor. The reason is lack of trust in protecting data in terms of confidentiality, availability and integrity. Some of the techniques for improving data security are

***a)*** ***Cryptography:*** Cryptography is one of the most employed practices to secure sensitive data from olden days. Every day new security algorithms were being proposed to improve security.

***b)*** ***Redundancy:*** Redundancy means copy of data. If Client's data is stored at one cloud resource and due to some reason if the data is lost then there will be huge damage for client who trusted the vendor. So, for safety purpose data should be copied to some other cloud resource too which reduces the risk of loss of data.

*c)* ***Disposal:*** Storing data redundantly in multiple cloud resources will reduce the risk of data loss but when user wants to destroy his data completely he don't want any redundant form of his data to exist. So destroying data completely without any copies of log references and registers is important.

*d)* ***Data Control:*** Data transfer to and from the cloud creates loss of control over redundancy, location and file systems etc.

- **Virtualization**

Virtualization technology changed the functionality of cloud computing technology. Virtualization became solution for many problems. Isolation of Virtual Machines, Hypervisor vulnerabilities etc provide better security.

*a)* ***Isolation:*** Problems arise even after isolating virtual machines because they share same resources even they are isolated which allows malicious content that causes data leakage and cross VM attacks.

*b)* ***Hypervisor Vulnerabilities:*** Using hypervisor VM's will be created which is having some very high vulnerability for security attacks.

*c)* ***Data Leakage:*** Leakage of data by malicious contents is possible while working with VM's and it is one important thing which one should look after.

*d)* ***VM Identification:*** Using hypervisor many VM's can be created on a single server. Identification of a particular VM should not be ambiguous; lack of control over identifying a VM or cross VM attacks will become a major security issue.

- **Governance**

Many companies report that they will lose administrative & security controls if they move to cloud technology.

**a)** ***Security Control:*** Insufficient Service level Agreements can lead to misconceptions over the security & administrative controls.

**b)** ***Lock-in:*** Occurs when the service providers are having lack of well established standards.

- **Compliance**

Compliance of Service availability & Audit capabilities must be very clear for both client and vendor.

**a)** ***Service Level Agreements:*** Service availability must be ensured properly

**b)** ***Audit:*** An automated API is needed for estimating performance of security and service availability.

**c)** ***Service Conformity:*** Based on the Agreements made the service should be available.

**d)** ***Legal issues:*** Judicial issues & Law must be taken care with respective to geographical regions because law may change from country to country.

**e)** ***Data Location:*** If data of client is held in multiple locations, then it can be exaggerated by certain law measures.

**f)** ***E-discovery:*** Data of all the customers will be stored in same hardware which will be affected due to the law investigation of one customer

## VI. Future Challenges of Cloud Computing

- ***Protocol Reaching***

Cloud computing is gaining importance in the IT industry day-by-day. There were many achievements currently made by cloud computing but there is a serious problem to be solved in cloud computing that is there is no universally accepted protocol. The transmission of data to and from the cloud is not that flexible today. To improve the performance a new protocol must be invented which should accepted universally and with such protocol the consumers and

the API's will be standardized which will lead to the enhanced service capability of cloud computing.

- ***Unpredictable Performance***

With the virtualization technique in cloud computing the virtual machine will share the processing and memory power in a much optimized manner. But coming to the I/O sharing there is a problem. Another problem in unpredictability is scheduling of virtual machines for some classes of batch processing programs, specifically for high performance computing.

- ***Data Security & Reliability***

In cloud computing security is the major burning issue to be solved; the cloud service provider must provide a tool which ensures that the environment of cloud which is shared by number of users is a safe place to store the data. Strict methods must be followed to prevent hacking of data and there must be a regular updated backup.

## VII. Conclusion

Present day cloud computing is becoming more popular because of its capability of providing cost saving and fast delivery of services. The cloud computing industry is analyzing to enhance the way of delivering its services to customers but it should also concentrate on the security issue which was becoming serious day-by-day. This paper analyzes different security issues in cloud computing. The results of a survey conducted by several organizations about the deployment and service models are discussed in this paper.

## VIII. References

[1] NIST "The NIST definition of cloud computing", [Online], Available: http://csrc.nist.gov/groups/SNS/cloud computing/ cloud-def-v15.doc, 2009.

[2] https://www.ibm.com/cloud-computing/learn-more/what-is-cloud-computing/

[3] Hassan, Qusay . "Demystifying Cloud Computing" (PDF). The Journal of Defense Software Engineering. CrossTalk. 2011 (Jan/Feb): 16–21. Retrieved 11 December 2014

[4] http://forwardthinking.pcmag.com/none/325351-when-big-companies-don-t-trust-cloud-computing

[5] V Raviteja Kanakala, V Krishna Reddy, K.Karthik. "Performance Analysis of Load Balancing Techniques in Cloud Computing Environment" in ICECCT, International Conference on Electrical, Computer and Communication Technologies, IEEE, March 2015.

[6] "Security Issues And Resource Planning In Cloud Computing", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 2 Feb 2013 Page No. 400-407, Dr Dwivedi, Dr Kushwaha.

[7] "Cloud Computing Benefits, risks and recommendations for information security", ENISA, December 2012.

[8] V Raviteja Kanakala, V Krishna Reddy *et a*l, "Issues to Adopt Cloud for IT Services" in the International Journal of Applied Engineering (IJAER) ISSN 0973-4562 Volume 9, Number 13 (2014) pp.2325-2334, April 2014.

[9] Voas.J, & Zhang, J.(March/April 2009) Cloud Computing: New Wine or Just a New Bottle? IEEE ITPro, pp.15–17.