# CLOUD COMPUTING A POTENTIAL TO CHANGE IT

***Sumanth S***
Assistant Professor, Department
of Computer Science,
Smt. V.H.D. Central Institute
of Home Science (Autonomous), Bengaluru.

***Yethiraj N G***
Assistant Professor, Department
of Computer Science,
Maharani's Science College
for Women, Bengaluru.

## ABSTRACT

*Cloud computing is an emerging technology in IT world. It is a set of IT services such as software's, applications and hardware resourcesthat are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Usually cloud computing services are delivered by a third party provider who owns the infrastructure.*

*To mention few advantages it includes scalability, resilience, flexibility, efficiency and outsourcing non-core activities. Cloud Computing initiatives could affect the enterpriseswithin two to three years as it has the potential to significantly change IT. The major issue and the most of the research are carried on the security issues which hampers thegrowth of cloud. This paper provides a survey of the security challenges focusing on the cloud computing types and the service delivery types.*

***Keywords: Cloud Computing, IT, infrastructure, Scalability,***

## INTRODUCTION

Cloud Computing is today's most inspiring technology in industry and in research. Cloud computing is a model forenabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing sources(e.g.,network, servers, storage, applications, and services) that can rapidly provisioned and released with minimal managementeffort or service provider interaction.[1] Cloud computing services are quickly becoming formal and integral members ofIT portfolio. Organizations are adopting cloud-based platforms which provides infrastructure and application services asa pay-per-use basic. Client organization are more concern with lack of security and it is the, most important reasonsorganizations are hesitating for adopting cloud services.[2] To make cloud computing adopted by users and industry, thesecurity concerns has to be rectified.

Cloud computing is an emerging technology which provides IT services and resources to the customers through public network specifically internet. The cloud computing services and infrastructure are mostly owned by a third party called cloud service providers. Cloud computing offers an innovative model for the organizations to use software applications, storage and processing capabilities of cloud without investing on the infrastructure. As compared to existing IT models, the cloud computing offers many advantages like scalability, flexibility, efficiency and non-core activities [3]. Despite these extraordinary benefits of cloud computing, the security is a major concern. According to the International Data Corporation (IDC) survey published in 2009, 74% IT managers and Chief Information Officers (CIOs) thinks that security and privacy issues is the main obstacle preventing organizations to adopt cloud computing services. In the same year a survey conducted by Garter that more than 70% Chief Technology Officers (CTOs) showed their concern about data security and privacy issues in cloud computing [4, 5].

### 2. Cloud Computing - Infrastructure

### 2.1. Different service delivery models of cloud computing

The cloud computing model is based on three service delivery models and three cloud deployment models [3, 4, 5, 6, and 7].

The three service delivery models are:

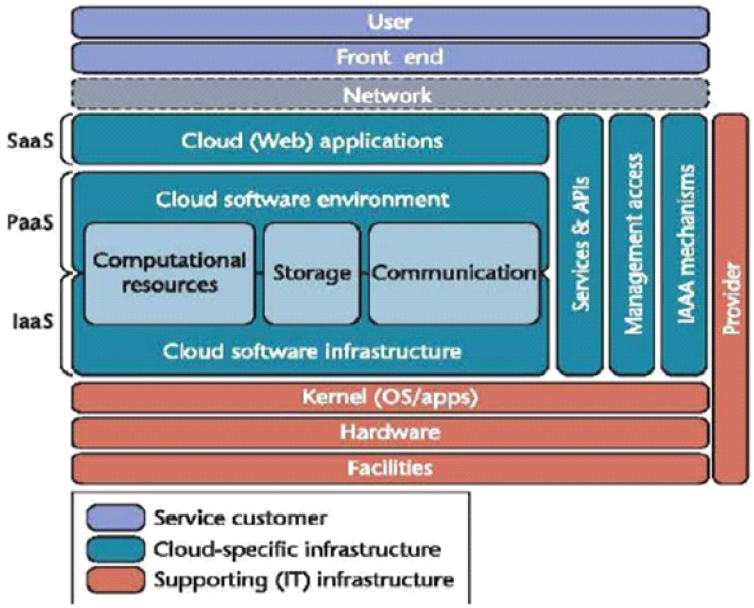


Fig.1 The cloud reference architecture

**Infrastructure as a service (IaaS)**:In this model the cloud providers offers the cloud services like hardware resources, storage and network infrastructure services. The virtualization is the base of this model. IaaS are provided by Amazon Ec2, Amazon S3, Rackspace Cloud Servers etc.[6,7]

**Platform as a service (PaaS)**:In this model the cloud service providers provide application development platform for the developers. They also deliver a set of APIs for the developers to develop and launch their own customized applications. They do not need to install development tools on their local devices and machines. PaaS providers are Google's Application Engine, Microsoft's Azure, etc.

**Software as a service (SaaS)**:This model facilitates the customers to access the applications hosted on the cloud. Instead of installing the applications on their own machines, the users access these applications installed on the cloud using their own browsers. Like Salesforce.com offers online CRM space, Google's Gmail, Google docs, Microsoft's online version of office BPOS (Business Productivity Online Standard Suite).This model can be hosted directly on the cloud or may be PaaS and IaaS.

**Data as a Service (DaaS)**
The delivery of virtualized storage on demand becomes a separate Cloud service - data storage service. Notice thatDaaS could be seen as a special type IaaS. The motivation is that on-premise enterprise database systems are often tied in a prohibitive upfront cost in dedicated server, software license, post-delivery services and in-house IT maintenance. DaaS allows consumers to pay for what they are actually using rather than the site license for the entire database. In addition to traditional storage interfaces such as RDBMS and file systems, some DaaS offerings provide table-style abstractions that are designed to scale out to store and retrieve a huge amount of data within a very compressed timeframe, often too large, too expensive or too slow for most commercial RDBMS to cope with. Examples of this kind of DaaS include Amazon S3, Google BigTable, and Apache HBase, etc.

### 2.2. Cloud Deployment Models

The cloud has three different deployment models and each model has its own benefits and trade-offs. There is also another model called community model but it is used in rare cases.

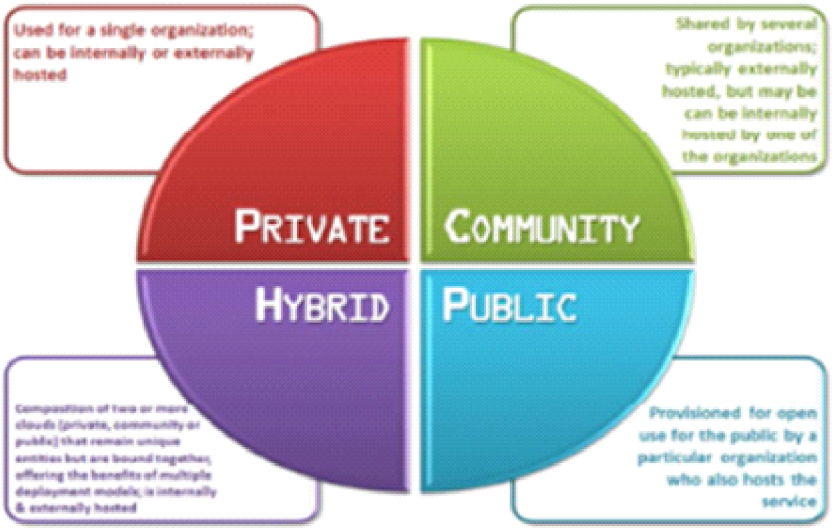


Fig.2Types of cloud's

**Private cloud**: This cloud is setup specifically for an organization within its own data center. The organizations manage all the cloud resources which are owned by them. The private cloud offers more security as compared to other two. Are dedicated to a particular organization which are managed internally or by third-party and hosted internally or externally like Amazon ( EC2). It is managed by the users or by a third party within or outside the premises.

**Public cloud**: This cloud is available to all the external users through internet who can register with cloud and can use cloud resources on a pay-per-use model. This cloud is not secure like private cloud because it is accessible to the internet users. Are offered by service providers for general public over the internet. Like Amazon, IBM's Blue Cloud, Google AppEngine, Windows Azure etc,. The general public can use the infrastructure available via internet.

**Hybrid cloud**: This is a type of private cloud which uses the resources of one or more public clouds. It is a mix of both private and public cloud. Organization can host critical data in private clouds and applications in public clouds which are less secure.

**Community cloud:** This cloud involves sharing infrastructure between organizations of same community like allgovernment organizations within same state.

**Virtual Private Cloud:** This cloud is mentioned by less sources and it consists on using Virtual Private Network (VPN) connectivity to create virtual private or semi-private clouds, resorting to secure pipes supplied by VPN technology and by assigning isolated resources to customers. A VPC seats on top of any model previously described, likewise a VPN that is built upon other networks. Hence, a VPC is a particular case of private cloud existing within any other. An example of this model is Amazon VPC

The five cloud services described above attract some highly significant amount of threats. This includes modification of data without proper backup, leading to data breaches or unauthorized access to sensitive data. In case of proper data backup being taken, it is vulnerable if it is not encrypted properly. Unsecured access to resources over the cloud may lead to unauthorized usage of service, platform or even an infrastructure of the provider or other users due to the associated disadvantages of virtualization.

Table 1 : Summary of the main characteristics of the cloud deployment models, regarding Ownership (Organization (O),

Third-Party (TP), or Both (B)), Management (O, TP, or B), Location (O_-site, On-site, or B), Cost (Low, Medium, or High),

and Security (Low, Medium, or High).

| Deployment Model | Ownership | Management | Location | Cost | Security |
|---|---|---|---|---|---|
| Public | TP | TP | Off-site | Low | Low |
| Private | O or TP | O or TP | On-site | High | High |
| Community | O or TP | O or TP | On-site | High | High |
| Hybrid | O and TP | O and TP | On-site and Off-site | Medium | Medium |
| VPC | B | B | B | B | High |

## 3. Data Security Issues

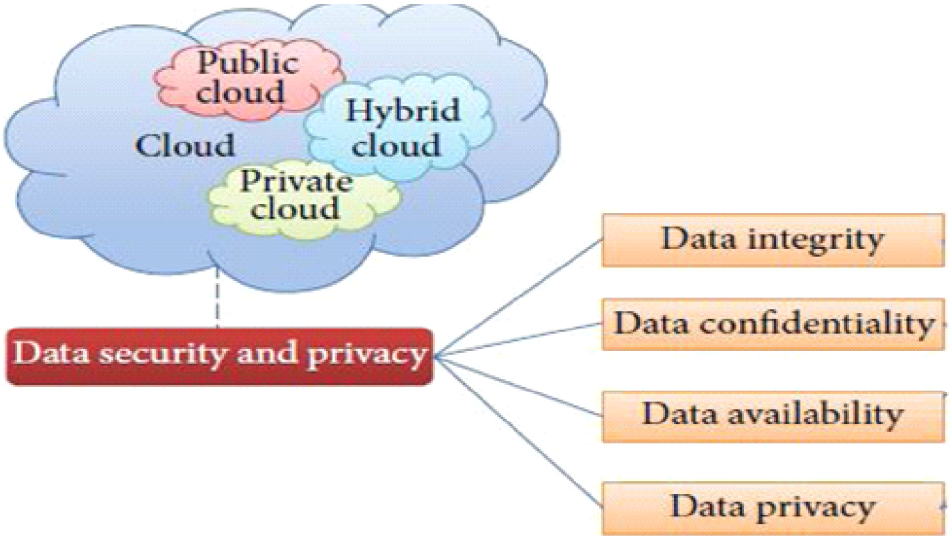


Fig.3 Various data security

### 1. Data Integrity

Integrity refers to the prevention of unauthorized modification of data and it ensures that data is of high quality, correct, consistent and accessible. After moving the data to the cloud, owner hopes that their data and applications are secure. It should be insured that the data is not changed after being moved to the cloud. It is important to verify if one?s data has been tampered with or deleted. Strong data integrity is the basis of all the service models such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Methods like digital signature, Redundant Array of Independent Disks (RAID) strategies etc. are some ways to preserve integrity in Cloud computing. The most direct way to enforce the integrity control is to employ cryptographic hash function. For example, a solution is developed as underlying data structure using hash tree for authenticated network storage [8].

### 2. Data Confidentiality

Prevention of the unauthorized disclosure of the data is referred as Confidentiality. Normally, Cloud works on public networks; therefore, there is a requirement to keep the data confidential the unauthorized entities. With the use of encryption and physical isolation, data can be kept secret. The basic approaches to attain confidentiality are the encrypting the data before placing it in a Cloud with the use of TC3 (Total Claim Capture & Control) [9].

### 3. Data Availability

Availability refers to the prevention of unauthorized withholding of data and it ensures the data backup through Business Planning Continuity Planning (BCP) and Disaster Recovery Planning (DRP). In addition, Availability also ensures that they meet the organization?s continuity and contingency planning requirements. Availability can be affected temporarily or permanently, and a loss can be partial or complete from Temporary breakdowns, sustained and Permanent Outages, Denial of Service (DoS) attacks, equipment failure, and natural calamities are all threats to availability [10]. One of the major Cloud service provider, AWS had a breakdown for several hours, which lead to data loss and access issues with multiple Web 2.0 services [11].

**4. Data Privacy:** As cloud computing involves exchange of data with users , other cloud servers there arechances of data leakage from cloud or unauthorized access to stored data. Now a day cloud servers mightcontains user's sensitive data so privacy is needed but not properly preserved.

**4. Key Security Challenges In Cloud Computing**

Security has been one of the most challenging issues for the IT executives particularly in cloud implementation. There exist numerous security anxieties that are preventing companies from captivating advantages of the cloud. Several studies, including the one by AmitSangroya et al. [12] quote security as the primary level confront for cloud users. In this section taxonomy related to cloud computing security has been presented.

Fig. 4 represents the schematic diagram showing the hierarchy of the cloud computing, with security challenges on both the cloud computing models: Deployment and Service models and also the issues related to Networks.The classification provided above reveals various common challenges under cloud computing. The Deployment model is classified further as Private, Public and Hybrid Cloud and the security issues of the same have been exposed in common. Further, the Service model is classified into the SaaS, PaaS and IaaS briefing its security challenges in common. The security challenges with respect to network is also shown as for any internet based service, network is considered as the backbone for cloud computing.

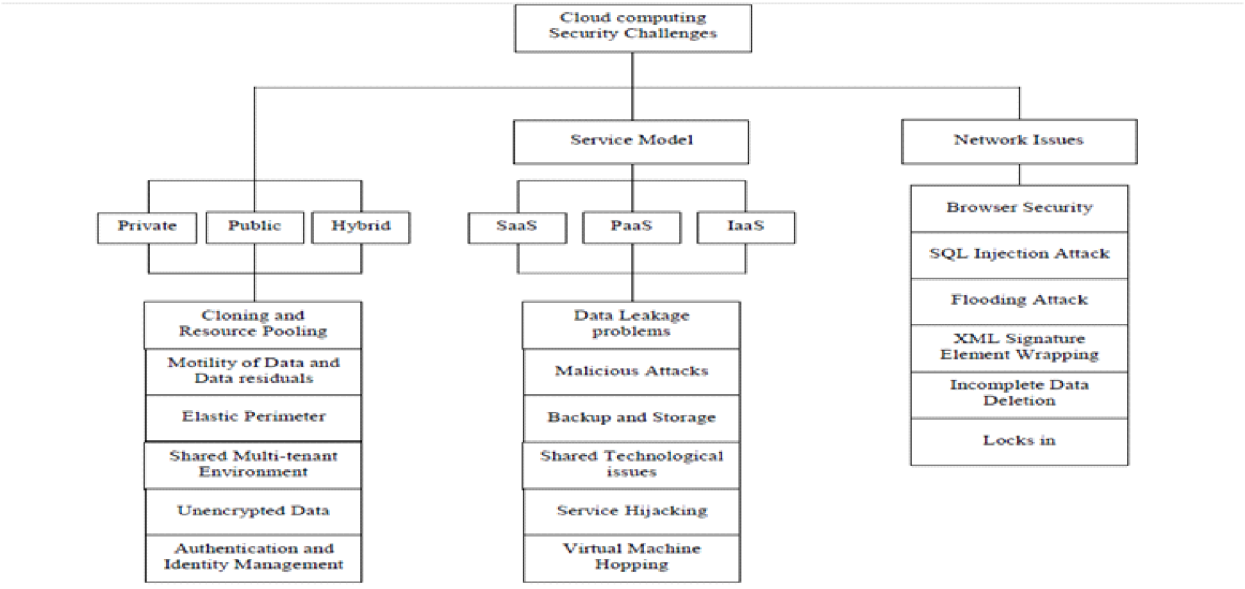


Fig 4. Classification of Security Challenge

**A. Deployment Models and its security challenges:**

There exist three basic types of deployment models, namely Private, Public and Hybrid clouds. Private cloud model is generally deployed within an organization and is limited only for the internal access by individuals of that organization. Public cloud model is employed by the organization for gaining access to various resources, web applications, and services over any of internet, intranet as well as extranet. Hybrid cloud is the combination of two or more clouds (public and/or private). It is an environment providing multiple service suppliers, both internal and external.

Various security challenges related to these deployment models are mentioned below:

- Cloning and Resource Pooling
- Motility of Data and Data residuals
- Elastic Perimeter
- Shared Multi-tenant Environment
- Unencrypted Data
- Authentication and Identity Management

**B. Service models and security challenges:**

Various cloud services like Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a

Service (IaaS) are delivered and used in real time over the cloud. Bhaskar Prasad Rimal et al. [13] have mentioned SaaS as a multi tenant platform which is commonly referred to as Application Service Provider aiding distribution of services across cloud users. While the PaaS provides the developers a platform to work with all the environments and systems for the developing, testing and deploying web applications through the cloud service. The computer infrastructure needed for this application to run on a particular platform is provided by IaaS which may give more flexibility and pay-as-you-go scheme.

According to John Viegga[14], the users of SaaS have to rely heavily on the cloud provider for security purposes without any assurance to the data protection of users. In PaaS, the cloud providers offer some controls to the users building applications on their platform, without ensuring them the threats with network or intrusion prevention. While with IaaS, the developers have a better control over the application. This addresses proper security and compliance.

Various security challenges with the service models are mentioned below:

- Data Leakage and consequent problems
- Malicious Attacks
- Backup and Storage
- Shared Technological issues
- Service Hijacking
- VM Hopping
- VM Mobility
- VM Denial of Service

**C. Network issues on Cloud:**

Cloud computing mainly depends upon internet and remote computers or servers in maintaining data for running various applications. The network is used to upload all the information. With the same aspect, H.B. Tabakki et al. [15] have stated security issues with network on cloud as a prime focus. It provides virtual resources, high bandwidth and software to the consumers on demand. But in reality, the network structure of this cloud faces various attacks and security issues like cloud malware injection attack, browser security issues, flooding attacks, locks-in, incomplete data deletion, data protection and XML signature element wrapping, which are explained further below.

- Browser Security
- SQL Injection Attack
- Flooding Attacks
- XML Signature Element Wrapping
- Incomplete Data Deletion
- Locks in

## 5. Applications

There are a few applications of cloud computing [16] as follows:

1) Cloud computing provides dependable and secure data storage center.
2) Cloud computing can realize data sharing between different equipments.
3) The cloud provides nearly infinite possibility for users to use the internet.
4) Cloud computing does not need high quality equipment for the user and it is easy to use.

## 6. CONCLUSION AND FUTURE WORK

Cloud computing is a most emerging IT trend. It offers more benefits to the users. Cloud computing faces number of security issues and challenges. In spite of the severallimitations and the need for better methodologies processes, cloud computing is becoming a hugely attractive paradigm, especially for large enterprises. Cloud Computing initiatives could affect the enterpriseswithin two to three years as it has the potential to significantly change IT. This study has surveyedvarioussecurity challenges in cloud computing environment withrespect to deployment model, service model and network issues. The work will be further extended to find the solutions for the security in cloud computing models.

## REFERENCES

[1] Mell, P., Grance, T. (2009) The NIST Definition of Cloud Computing Version 15. NIST
[2] The Forrester Wave™: Public Cloud Platform Service Providers' Security, Q4 2014 by AndrasCser and Ed Ferrara, November 17, 2014

[3] S. O. Kuyoro, F. Ibikunle and O. Awodele, "Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), vol. 3, Issue 5, (2011).
[4] K. opovi and Z. Hocenski, "Cloud computing security issues and challenges", MIPRO, 2010 Proceedings of the 33rd International Convention, (2010)May 24-28.
[5] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering (ICCSEE), (2012)March 23-25.
[6] M. Al Morsy, J. Grundy and I. Müller, "An Analysis of The Cloud Computing Security Problem", In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, (2010), November 30.
[7] Soeung-Kon, J. -H. Lee and S. W. Kim, "Mobile Cloud Computing Security Considerations", Journal of Security Engineering, no. 9, (2012)April.
[8] Yumerefendi, A.R., Chase, J.S., "Strong accountability for network storage". ACM Trans. Storage (TOS), Volume 3 Issue 3, October 2007, pp.382-401.
[9] Minqi Z; Rong Z; Wei X; Weining Q; Aoying Z, "Security and Privacy in Cloud Computing: A Survey", Sixth international conference on Semantics Knowledge and Grid (SKG), Nov. 1-3 ,2010, pp. 105.
[10] JansenWayne, GranceTimothy, "Guidelines on security and privacy in public Cloud computing", NIST, Special Publication 800-144, Dec 2011, pp.35
[11] KashifMunir, SellapanPalaniappan, "Secure Cloud Architecture", Advanced Computing: An International Journal (ACIJ), Vol.4, No.1, January 2013, pp.13.
[12] AmitSangroya, Saurabh Kumar, JaideepDhok, and VasudevaVarma, "Towards Analyzing Data Security Risks in Cloud Computing Environments", Springer-Verlag Berlin Heidelberg 2010, pp. 255-265.
[13] Bhaskar Prasad Rimal, Eunmi Choi, Ian Lumb, "A Taxonomy and Survey of Cloud Computing Systems", 978-0-7695-3769-6/09, IEEE, pp: 44 – 51.
[14] John Viega, "Cloud Computing and the Common Man", IEEE, 0018-9162/09, pp: 106 – 108.
[15] H. Takabi, J.B.D. Joshi, and G.-J. Ahn, "SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments," Proc. 1st IEEE Int'l Workshop Emerging Applications for Cloud Computing (CloudApp 2010), IEEE CS Press, 2010, pp. 393–398.
[16] S. Zhang, S. F. Zhang, X. B. Chen, and X. Z. Huo, "Cloud Computing Research and Development Trend," In Proceedings of the 2010 Second International Conference on Future Networks (ICFN '10). IEEE Computer Society, Washington, DC, USA, pp. 93-97. DOI=10.1109/ICFN.2010. 58.