International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 3, Number 8 (2013), pp. 771-778

http://www. irphouse.com /ijict.htm

# Cloud Computing: Advantages and Security Challenges

**Satyakam Rahul[1] and Sharda[2]**

[1]*Department of Computer Science and Information Technology*
*Kebbi State University of Science and Technology, Nigeria.*
[2]*Department of Computer Science, Guru Jambheswar University, Hisar, India.*

## Abstract

Cloud Computing is a new computing paradigm that has a lot of advantages due to its ability to reduce cost associated with computing while increasing flexibility and scalability for computers. Cloud Computing is a new concept of providing scalable and virtualized resources, bandwidth, software and hardware on demand to consumers. however, security issues especially data security and privacy protection issues, remain the primary concern for its adoption. This paper outlines the meaning, scope, the main security risks and privacy issues of the cloud computing environment. Finally, the paper provides an analysis on data security and privacy protection issues associate with Cloud Computing and possible responses.

**Keywords**: Cloud Computing, Cloud Platform, Data Privacy, Data Security, Models of Cloud Computing.

## 1. Introduction

Cloud Computing can be defined as a computing model for enabling convenient on-demand network access to share pool of configurable computing resources [1] e.g., networks, services, storage, applications that can be rapidly provisioned and released with minimal management effort or service provider interaction. Five essential characteristics [2] of Cloud Computing can be delineated as following-

i. On demand self service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without human interaction with each service provider.

ii. Broad network access: Capabilities are available over the network and accessed through standard mechanism that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops )

iii. Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

iv. Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. The capabilities available to the consumer for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

v. Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. Cloud Computing is a network based environment that focuses on sharing computations or resources. It refers to both the application delivered as services over the internet and the hardware and software in the datacenters that provide those Services. Clouds offer an opportunity to perform intense computation and large scale data storage without introducing a significant load on devices that are designed to be minimally noticeable.

The use of clouds can enable hardware designer to create more compact devices that are less obtrusive to users since there is less need for powerful processing and large storage hardware [3]. Compared with traditional IT models the cloud computing has many advantages. But from the consumer prospective, cloud computing security concerns remain a major problem for its adoption. According to a survey carried out by Gartner [7], more than 70% of Chief Technical Officers believed that the primary reason for not using cloud computing services is that of the data security and privacy concerns.

## 2. Models of Cloud Computing

Cloud Services can be provided into three fundamental categories - Software as a Service (SaaS), Platform as a service (PaaS), and Infrastructure as a Service(IaaS). IaaS is the most basic and each higher models abstract from the details of the lower models. In 2012 network as a service (NaaS) and communication as a service (CaaS) were officially included by ITU(International Telecommunication Union) as part of the basic cloud computing models, recognized service categories of a telecommunication – centric cloud ecosystem.

### 2.1 Software as a Service

Sometimes it is also referred to as “Software on demand”. It is a process by which application service provider supplies different software applications over the Internet. With SaaS, a provider licenses an application to customer either as a service on demand through a subscription or sometimes at no charge. This makes the customer free from installing and operating the application on own computer [4]. The users' client machines require no installation of any application-specific software - cloud applications run on the server (in the cloud). SaaS is scalable, and system administration may load the applications on several servers. In the past, each customer would purchase and load their own copy of the application to each of their own servers, but with SaaS the customer can access the application without installing the software locally. SaaS typically involves a monthly or annual fee per user so price is scalable and adjustable if users are added or removed at any point. Some examples of SaaS include - Google Apps, Microsoft office 365, GT Nexus, Marketo and Trade Card.

### 2.2 Platform as a Service

In the PaaS model, cloud providers deliver a computing platform typically including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. The user doesn’t manage the infrastructure (including network, server, operating systems and storage) but he controls deployed applications and possibly their configuration. Platform as a Service is an outgrowth of Software as a service. PaaS has several advantages for developers .With PaaS, Operating system features can be changed and upgraded frequently. Some examples of PaaS include - Force.com, OrangeScape, AWS Elastic Beanstalk, Cloud Foundry, Heroku, Google App Engine, Microsoft Azure.

### 2.3 Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) refers to the sharing of hardware resources for executing services using Virtualization technology .It offers basic infrastructure on demand services and using Application programming Interface(API) for interactions with hosts, switches, and routers, and the capability of adding new equipment in a simple manner. The user has nothing to do with the hardware in the cloud infrastructure but he controls the operating system and deployed application. The service provider is responsible for running and maintain it. To deploy their applications, cloud users install operating-system images and their application software on the cloud infrastructure. In this model, the cloud user patches and maintains the operating systems and the application software. Cloud providers typically bill IaaS services on a utility computing basis: cost reflects the amount of resources allocated and consumed. Examples of IaaS include : Amazon Elastic Cloud Computing, DynDns, Google Compute Engine, HP Cloud, iland, Joyent, Rackspace Cloud, Ready Space Cloud Services

### 2.4 Network as a Service (NaaS)

A category of cloud services where the capability provided to the cloud service user is to use network/transport connectivity services and/or inter-cloud network connectivity services[5]. NaaS involves the optimization of resource allocations by considering network and computing resources as a unified whole.Traditional NaaS services include flexible and extended VPN, and bandwidth on demand. NaaS concept materialization also includes the provision of a virtual network service by the owners of the network infrastructure to a third party (VNP – VNO) [6].

### 2.5 Communications as a Service (CaaS)

It is an outsourced enterprise communications solution that can be leased from a single vendor. Such communications can include voice over IP(VoIP or Internet telephony), instant messaging(IM), collaboration and videoconference applications using fixed and mobile devices. CaaS has evolved along the same lines as Software as a Service (SaaS). The CaaS vendor is responsible for all hardware andsoftware management and offers guaranteed Quality of Service .CaaS allows businesses to selectively deploy communications devices and modes on a pay-as-you-go, as-needed basis. This approach eliminates the large capital investment and ongoing overhead for a system whose capacity may often exceed or fall short of current demand. CaaS offers flexibility and expandability that small and medium-sized business might not otherwise afford, allowing for the addition of devices, modes or coverage on demand. The network capacity and feature set can be changed from day to day if necessary so that functionality keeps pace with demand and resources are not wasted. There is no risk of the system becoming obsolete and requiring periodic major upgrades or replacement.

## 3. Types of Cloud deployment models

### 3.1 Public Cloud

Public cloud applications, storage, and other resources are made available to the general public by a third party service provider. These clouds are fully hosted and managed by the cloud providers .These services are free or offered on a pay-per-use model. Since consumers have little control over the infrastructure so a process which requires very powerful security are not good for it .In this model no access restriction can be applied and no authorization and authentication techniques can be used. Generally, public cloud service providers like Amazon AWS, Microsoft and Google own and operate the infrastructure and offer access only via Internet (direct connectivity is not offered).

### 3.2 Private Cloud

Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally. Undertaking a private cloud project requires a significant level and degree of engagement to virtualize the business environment, and it will require the organization to reevaluate decisions about existing resources. It is more expensive and secured when compared to public cloud. In the private cloud the cloud service providers and the clients have optimized control of the infrastructure and improved security, since user's access and the network used are restricted.

### 3.3 Hybrid Cloud

Hybrid cloud is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models. By utilizing "hybrid cloud" architecture, companies and individuals are able to obtain degrees of fault tolerance combined with locally immediate usability without dependency on internet connectivity. Hybrid cloud architecture requires both on-premises resources and off-site (remote) server-based cloud infrastructure[2]. The major drawback to the hybrid cloud is the difficulty in effectively creating and governing such a solution. Services from different sources must be obtained and provisioned as if they originated from a single location, and interaction between private and public components cam make the implementation even more complicated. An example of a Hybrid Cloud includes Amazon Web Services(AWS).

### 3.4 Community Cloud

It is something like infrastructure shared by several organizations for a common cause and may be managed by them or a third party service provider. These clouds are based on an agreement between related organization. Facebook is one of the examples of community cloud.

## 4. Security threats in cloud computing

There are many security threats with cloud computing because it is comprised of several technologies like databases, operating systems, different networks, transaction management, virtualization etc. Therefore security issues related with these system and applications are applicable to cloud computing as well. According to Gardener [7], before making a choice of cloud vendors, users should ask the vendors for seven specific safety issues, viz. privileged user access, regulatory compliance, data location, data of cloud computing [8]. Following are the main security issues related with cloud computing- segregation, recovery, investigative support and long term viability. Cloud computing security is an evolving sub – domain of computer security, network security, and more broadly information security [2]. It also refers to a broad set of policies, technologies, and controls deployed to protect data, application and the associated infrastructure

i. Administrative access & Data ownership – In cloud computing administrative access are done through internet and this increases the risk. It is very important to control administrative access to data and monitor the access to maintain protocols. Data in the cloud is globally distributed which brings the issue of jurisdiction and privacy Organizations stand a risk of not complying with government policies [9]. There should be strong policy regarding Data ownership and organizations must comply government policies.

ii. Privacy of data – Data in the cloud is globally distributed. The user doesn't have information about the location of data and they don't have any control over physical access mechanism to that data. The concept of privacy is very different in different countries, culture and jurisdictions. There is also the question of whose jurisdiction the data falls under, when an investigation occurs .In a distributed system ,there are multiple databases and multiple applications. Governments should have at least a minimum common policy to handle this kind of situations.

iii. Transmission of data – In cloud environment data is sent from one place to another place. Encryption technique is used to for data during transmission but most of the data is not encrypted in the processing time and to process the data for any application it must be unencrypted. An attacker can find a place between communication path. The attacker can change the communication.

iv. Sharing of data – Data sharing is expanding the use of the data. The data owners can authorize the data access to one party and in turn the party can further share the data to another party. This sharing can create a serious problem like leakage of data to an unauthorized person. Therefore during the data sharing especially when shared with a third party, the data owners need to consider whether the third party continues to maintain the original protection measures and usage restriction .

v. Data Integrity : Data can corrupt at any stage and with any type of media .Data integrity can be easily achieved in a standalone system with a single database .Data integrity in such a system is maintained via database constraints. Data generated by cloud computing are kept in the cloud. So, it is very difficult to check integrity of data by user because the user has no control over data and their location .

vi. Key Management – The common solution for data confidentiality is date encryption. In order to ensure the effectiveness of encryption, there needs to consider the use of both encryption and key strength. A huge amount of data is stored by the user and it is difficult to encrypt large amount of data. it also requires fast processing speed and good computational efficiency. Encryption and decryption raises the issue of key management. who is responsible for key management. Ideally it is the owner of data but cloud users don't have much expertise to manage the keys, they normally trust the key management of the cloud providers. As the cloud providers need to maintain keys for a large number of users, key management becomes more difficult .

vii. Destruction of data – When data is no longer is required, it is supposed to be destroyed completely. Due to physical characteristics of storage medium, the data deleted may still exist and can be restored. This may result in disclose of sensitive data.

## 5. Possible solutions for security threat in Cloud Computing

The problem of key management is a big issue. The Organization for the Advancement of structured Information Standards (OASIS) key management Interoperability Protocol is trying to solve such issues [11]. About data destruction US Department of defense has some guidelines and method but it doesn’t explain how these methods are to be achieved [12].

Mowbray [13] proposed a client based privacy management tool. It provides a model to help users to control the storage and use of their sensitive information in the cloud. Randike Gajanayake proposed a privacy protection framework based on information accountability (IA) components [13].

## 6. Conclusion

Cloud computing is a new and emerging information technology that changes the way IT architectural solutions are put forward by means of moving towards the theme of virtualization of data storage, local networks as well as software. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human’s life easier. Although cloud computing has many advantages there are still many security problem, therefore one must be very careful to understand the limitations and security risks posed in utilizing these technologies. Data Security and privacy protection issues are the primary problem. The biggest security problem is the sharing of resources. This paper has highlighted all these issues of cloud computing. Cloud Security Alliance is a nonprofit organization formed to promote the use of best practice for providing security assurance within cloud computing. Cloud computing has many advantages but it doesn’t mean that all business IT needs to move to cloud in addition, As a result moving to cloud computing requires to consider several parameters and most important of them is security.

## 7. Acknowledgement

Authors are thankful to Kebbi State Univ. of Sci.& Tech., Nigeria for providing all essential infrastructural and financial assistance for this research.

## References

[1] Definition of cloud Computing, National Institute of Standard and Technology, V15, http:// csrc.nest.gov/groups/SNS/cloudcomputing/cloud-def-V15.doc

[2] http://en.wikipedia.org/wiki/File:Cloud_computing.svg

[3] Challenges in Securing the Interface between the cloud and pervasive systems. 106-110 1st IEEE Per Com workshop on Pervasive Communities and Service Control

[4] R.L. Grossman “The case for cloud computing” IT professional, Vol(2) ,P 23-27,2009

[5] "ITU Focus Group on Cloud Computing - Part 1". International Telecommunication Union (ITU) TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU. http://www.itu.int/en/ITU-T/focousgroups/cloud/Documents

[6] Network Vertulization Opportunity and challenges, Eurescom. http://archive.eurescom.eu/~pub/deliverables/documents/P1900-series/P1956/D1/P1956-D1.pdf

[7] Gartener: Seven cloud-computing security risks. InfoWorld.2008-07-02. http://www.infoworld.com/d/security-central/gartener-seven-cloud-computing-security-risks-853.

[8] Cloud computing security, http://in.wikipedia.org/wiki/cloud_computing_security

[9] Ronald L.Krutz, Russell Vines ”Cloud Security A Comprehensive Guide to secure Cloud Computing”, Willey Publishing, inc.,2010

[10] ”OECD Guidelines on the protection of Privacy and Transborder Flows of Personal Data ”at http://www.oecd.org/document/

[11] ”OAIS Key Management Interoperability protocol (KMIP) “ www.oais.org/committees / tc_home.php?ug_abbrev_kmip

[12] DoD “ National Industrial Security Program operating Manual”

[13] Randike Gajanayake, Renato Iannella and Tony Sahama “Sharing with care an Information Accountability perspective “ Internet computing, IEEE, Vol15 ,PP 31-38,July- Aug 2011.