An Overview of Cloud Computing Delivery Models: Security Issues and Challenges

Aluko T.S[1], Ayannusi A.O[2], Olusanya O.J[3], Oloyede O.E[4], Ebisin A.F[5]
Ogun State Institute of Technology Igbesa, Computer Science Department [1,5]
Ogun State Institute of Technology Igbesa, Cisco Department [2,3,4]
aluko.temitope@ogitech.edu.ng[1] *ayannusi.adebowale@ogitech.edu.ng[2],*
olusanya.olabanji@ogitech.edu.ng[3], oloyede.emmanuel@ogitech.edu.ng[4]
ebironke16@gmail.com[5]
+2348026262580, +2349035257874, +2348035023301, +2347066183340, +2348033529685

ABSTRACT

Cloud computing is a model for enabling service user's ubiquitous, convenient and on demand network access to a shared pool of configurable computing resources e.g. networks servers and storage applications. It is widely believed that Cloud computing is one of the newest technology and its benefits cannot be overemphasized. Despite the trumpeted business and technical advantages of cloud computing, security is a key concern in cloud computing most especially SaaS. In this paper we review a study of different security issues and challenges that could occur in a cloud environment. We also present as brief overview of cloud service models and also compare them. Few security and challenges that could occur in a cloud environment is given

Keywords: Cloud, SaaS, Networks, Security, Computing

1. BACKGROUND TO THE STUDY

A few years ago, abstract shapes of cloud were used todenote the internet and cyberspace. Afterwards the cloud has been utilized to represent a more specific idea, which is the Cloud Computing. The expansion and evolution ofthe electronic services requires conti nuous improvementin terms of infrastructure. Cloud computing offers a relatively low- cost scalable alternative to in-house infra-structure, both in hardware and software. [6]. Cloud computing is a network-based environment that focuses on sharing computations and resources. Actually, cloud computing is defined as a pool of virtualized computer resources.

Generally, Cloud providers use virtualization technologies combined with self-service abilities for computing resources via network infrastructures, especially the Internet and multiple virtual machines are hosted on the same physical server. Based on virtualization, the cloud computing paradigm allows workloads to be deployed and scaled-out quickly through the rapid provisioning of Virtual Machines or physical machines.[4]

A cloud computing platform supports redundant, self-recovering, highly scalable programming models that allow workloads to recover from many inevitable hardware/software failures. Therefore, in clouds, costumers only pay for what they use and do not pay for local resources, such as storage or infrastructure.[8]. Cloud computing is a general term for anything that involves delivering hosted services over theInternet. It is an emerging computing technology that uses the internet and central re mote servers to maintaindata.

This system is very helpful for different users so that they can e asily use the system without any externalsupport to software and hardware. They can also acc ess their personal files at any computer on internet. Thistechnology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth.[9] The primary motivation to move towards the cloud provider is reducing cost, responsibilities to maintain the resources, but not the responsibility towards security and privacy. [1,3]

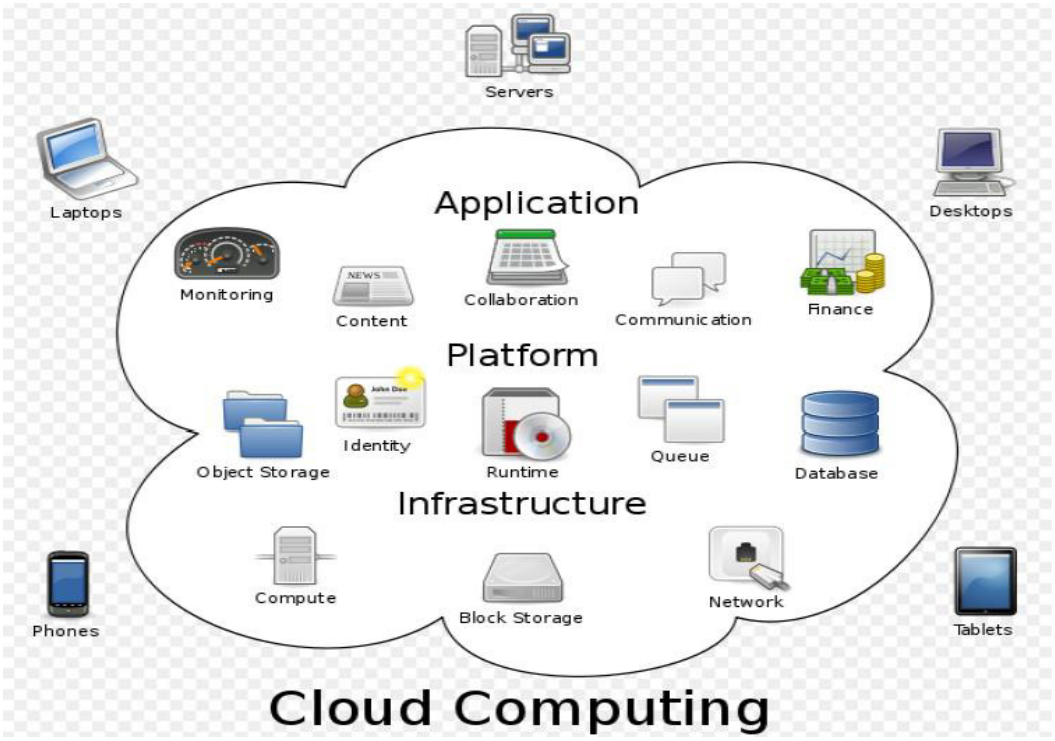


Figure 1: Cloud Computing Scenario

We are entering into a new era of computing, and it's all about the—cloud". This immediately brings up several important questions, which deserve thoughtful answers:—what is cloud computing?"—Is it real, or just another buzzword?" And most important,—How does it affect me?" Cloud computing as the dynamic provisioning of IT capabilities (hardware, software, or services) from third parties over a network. The term cloud computing refers to the delivery of scalable IT resources over the Internet, as opposed to hosting and operating those resources locally, such as on a college or university network. Those resources can include applications and services, as well as the infrastructure on which they operate.[1,5] By deploying IT infrastructure and services over the network, an organization can purchase these resources on an as -needed basis and avoid the capital costs of software and hardware. The coming shift to cloud computing is a major change in our industry. One of the most important parts of that shift is the advent (The coming or arrival, especially of something extremely important) of cloud platforms. As its name suggests, this kind of platform lets developers write applications that run in the cloud, or use services provided from the cloud, or both. Different names are used for this kind of platform today, including on -demand platform and platform as a service (PaaS).[1] Whatever it called, this new way of supporting applications has great potential.

1.1 Purpose of Cloud Computing Service Model

In practice, cloud service providers tend to offer services that can be grouped into three categories: software as a service, platform as a service, and infrastructure as a service. These categories group together the various layers with some overlap.

Cloud Software as a Service: The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. Applications can be accessed by different devices through a client interface such as a browser (like browser based email).

Cloud Platform as a Service: capability provided is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the providers.[3]

SaaS and PaaS both make it so that the user isn't bothered with managing or controlling the underlying cloud infrastructure, including network, servers, operating systems, storage or even individual application capabilities.

Cloud Infrastructure as a Service: Capability to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.[3]

1.2 Cloud Computing Security Issues and Challenges

laaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service) are three general models of cloud computing. Each of these models possesses a different impact on application security. However, in a typical scenario where an application is hosted in a cloud, two broad security questions that arise are:

- How secure is the Data?
- How secure is the Code?

Cloud computing environment is generally assumed as a potential cost saver as wen as provider of higher service quality. Security, Availability, and Reliability is the major quality concerns of cloud service users. [Gem et. al.], suggests that security in one of the prominent challenge among all other quality challenges. [9]

1.3 Security Challenges In Cloud Environments

In spite of security advantages, cloud computing paradigm also introduces some key security challenges. Here we discuss some of these key security challenges:

- **Data Location:** In general, cloud users are not aware of the exact location of the datacenter and also they do not have any control over the physical access mechanisms to that data. Most well-known cloud service providers have datacenters around the globe. Some service providers also take advantage of their global datacenters. However, in some cases applications and data might be stored in countries, which can judiciary concerns. For example, if the user data is stored in X country then service providers will be subjected to the security requirements and legal obligations of X country. This may also happen that a user does not have the information of these issues.[9,4]
- **Investigation:** Investigating an illegitimate activity may be impossible in cloud environments. Cloud services are especially hard to investigate, because data for multiple customers may be co -located and may also be spread across multiple datacenters. Users have little knowledge about the network topology of the underlying environment. Service provider may also impose restrictions on the network security of the service users.[5]
- **Data Segregation:** Data in the cloud is typically in a shared environment together with data from other customers. Encryption cannot be assumed as the single solution for data segregation problems. In some situations, customers may not want to encrypt data because there may be a case when encryption accident can destroy the data.
- **Long-term Viability:** Service providers must ensure the data safety in changing business situations such as mergers and acquisitions. Customers must ensure data availability in these situations. Service provider must also make sure data security in negative business conditions like prolonged outage etc.
- **Compromised Servers:** In a cloud computing environment, users do not even have a choice of using physical acquisition tools. In a situation, where a server is compromised; they need to shut their servers down until they get a previous backup of the data. This will further cause availability concerns.
- **Regulatory Compliance:** Traditional service providers are subjected to external audits and security certifications. If a cloud service provider does not adhere to these security audits, then it leads to a obvious decrease in customer trust.
- **Recovery:** Cloud service providers must ensure the data security in natural and man-made disasters. Generally, data is replicated across multiple sites.[9,11]

2. STATEMENT OF PROBLEM

There is a number of security issues associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing Software-, Platform-, or Infrastructure -as -a -Service via the cloud) and security issues faced by their customers. Security controls in cloud computing are, for the most part, no different than security controls in any IT environment. Cloud computing may present different risks to an organization than traditional IT solutions. Cloud computing is about gracefully losing control while maintaining accountability even if the operational responsibility falls upon one or more third parties. While cloud security concerns can be grouped into any number of dimension:, these dimensions have been aggregated into three general areas Security and Privacy, Compliance, and Legal or Contractual Issues. [6]

3. OBJECTIVE

The main objective of this study is to reviews some Cloud services models and security challenges faced by cloud computing. Current cloud service providers operate very large systems. They have sophisticated processes and expert personnel for maintaining their systems, which small enterprises may not have access to. As a result, there are many direct and indirect security benefits for the cloud users. Here we present some of the key security benefits of a cloud computing environment:

1 Data Centralization
2 Incident Response:
3 Forensic Image Verification Time
4 Logging

4. METHODOLOGY

4.1 Cloud Computing Deployment Service Models

Cloud computing architects provides three basic service models

- Public cloud
- Private cloud
- Hybrid cloud
- Community Cloud

IT organizations can choose to deploy applications on public, private, or hybrid clouds, each of which has its trade-offs. The terms public, private, and hybrid do not dictate location. While public clouds are typically -out there" on the Internet and private clouds are typically located on premises, a private cloud might be hosted at a Collocation (share or designate to share the same place) facility as well. A number of considerations with regard to which cloud computing model they choose to employ, and they might use more than one model to solve different problems.[7,9] An application needed on a temporary basis might be best suited for deployment in a public cloud because it helps to avoid the need to purchase additional equipment to solve a temporary need.

Likewise, a permanent application, or one that has specific requirements on quality of service or location of data might best be deployed in a private or hybrid cloud.

Public clouds: Public clouds are ran by third parties, and applications twin dittetent customers are likely to be mixed together on the cloud's servers, storage systems, and networks. Public clouds are most often hosted away from customer premises, and they provide a way to reduce customer risk and cost by providing a flexible, even temporary extension to enterprise infrastructure. If a public cloud is implemented with performance, security, and data locality in mind, the existence of other applications running in the cloud should be transparent to both cloud architects and end users. Portions of a public cloud can be carved out for the exclusive use of a single client, creating a virtual private datacenter. Rather than being limited to deploying virtual machine images in a public cloud, a virtual private datacenter gives customers greater visibility into its infrastructure.[6] Now customers can manipulate not just virtual machine images, but also servers, storage systems, network devices, and network topology.

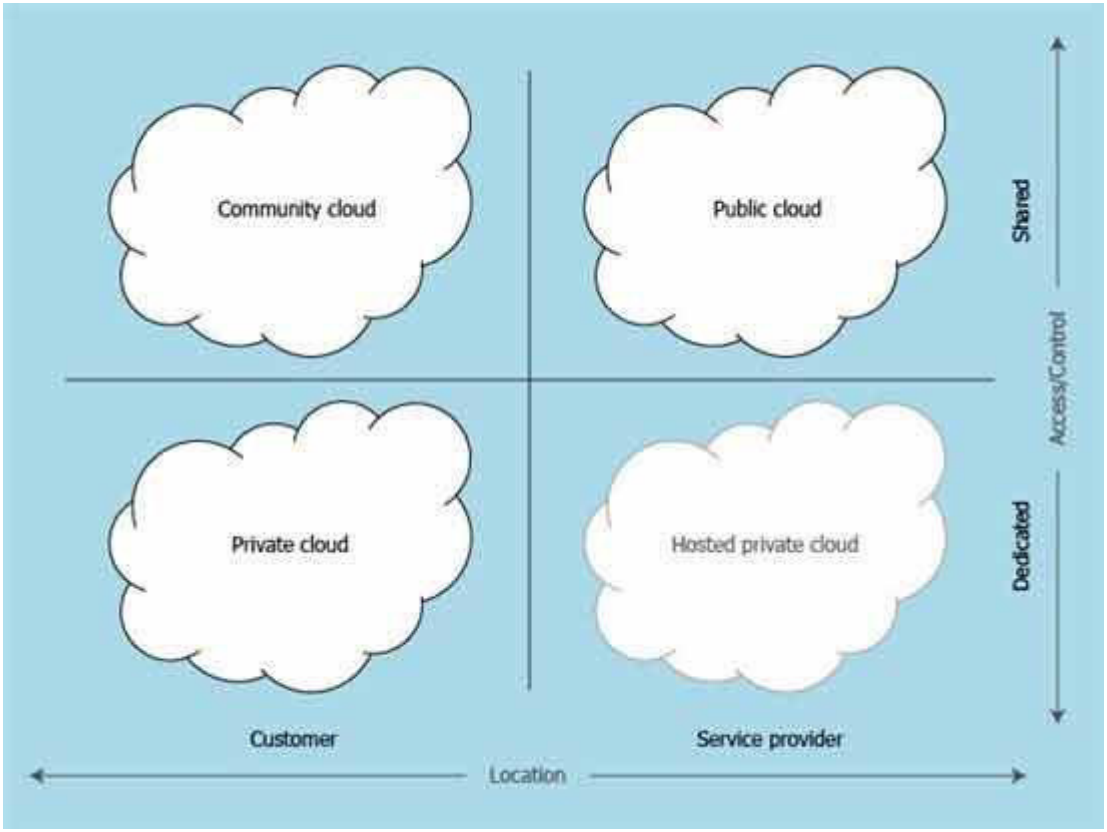
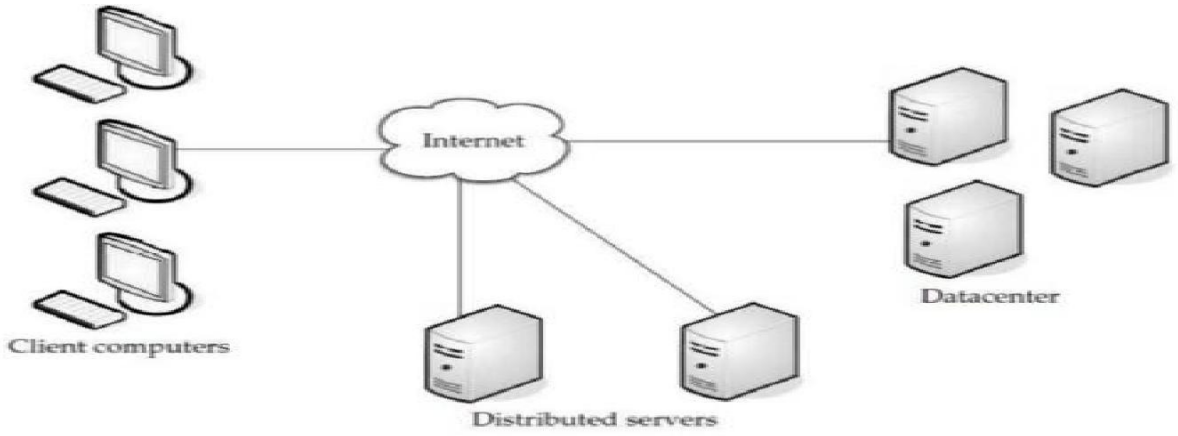


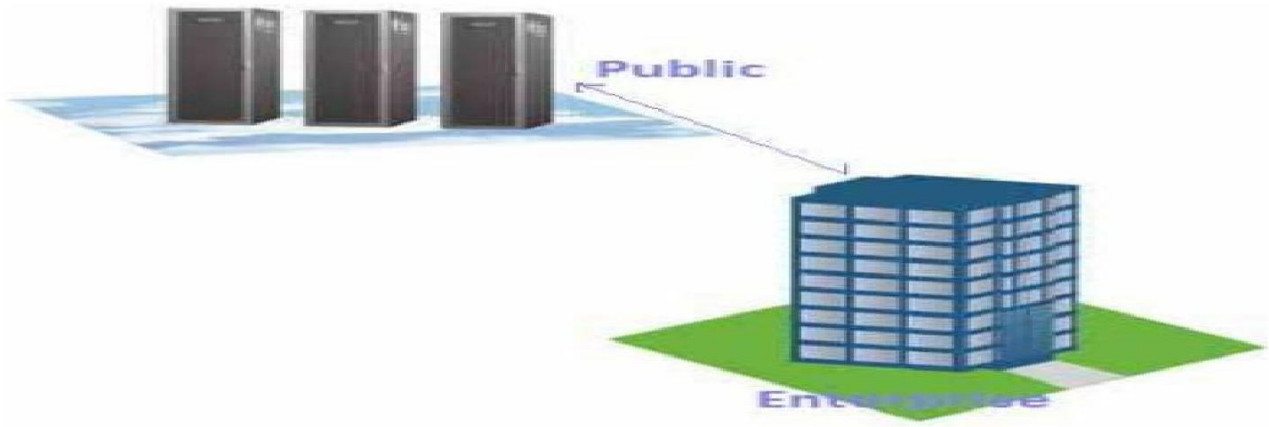
Figure 2:Cloud computing deployment models

Private clouds: Private clouds are built for the exclusive use of one client, providing the utmost control over data, security, and quality of service. The company owns the infrastructure and has control over how applications are deployed on it. Private clouds may be deployed in an enterprise data centre, and they also may be deployed at a collocation facility.[4] Private clouds can be built and managed by a company's own IT organization or by a cloud provider. In this -hosted private" model, a company such as Sun can install, configure, and operate the infrastructure to support a private cloud within a company's enterprise datacenter. This model gives companies a high level of control over the use of cloud resources while bringing in the expertise needed to establish and operate the environment.

Hybrid clouds: Hybrid clouds combine both public and private cloud models. They can help to provide on -demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to maintain service levels in the face of rapid workload fluctuations. This is most often seen with the use of storage clouds to support Web 2.0 applications. A hybrid cloud also can be used to handle planned workload splices. Sometimes called-surge computing," a public cloud can be used to perform periodic tasks that can be deployed easily on a public cloud.[10] Hybrid clouds introduce the complexity of determining how to distribute applications across both a public and private cloud. Among the issues that need to be considered is the relationship between data and processing resources. If the data is small, or the application is stateless, a hybrid cloud can be much more successful than if large amounts of data must be transferred into a public cloud for a small amount of processing.

Community clouds: In Community Cloud the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, or compliance considerations). It may be managed by the organizations or a third party and may exist on -premises or off -premises.





Public Cloud Model

Figure 3: Private Cloud Model

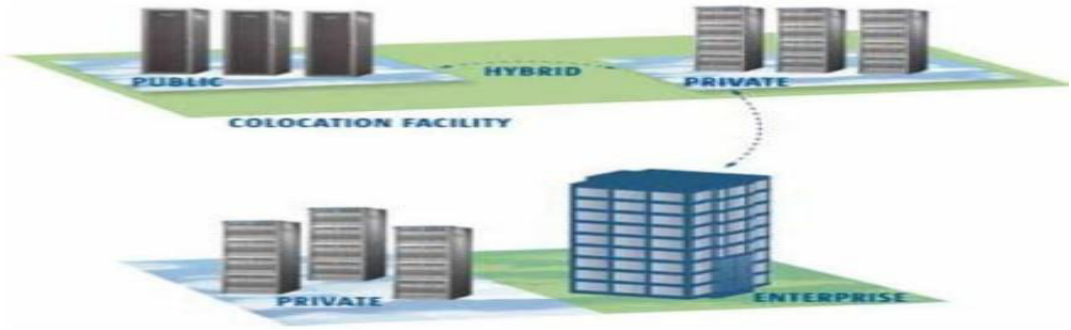


Figure 4: Hybrid Cloud Model

5. ANALYSIS OF CLOUD COMPUTING DEPLOYMENT MODELS

Table1: showing different types of deployment models

FUNCTIONALITY	PUBLIC	PRIVATE	HYBRID	COMMUNITY
Ease of Use and Configuration	High	Low	Moderate	moderate
Cost	Low	High	moderate	low
Security	Poor	Excellent	Good	moderate
Dedicated hardware	NO	Yes	Depend on contract	No
Managed by	Cloud service provider	Internal organization	mixed	Shared
Owner of Infrastructure	Cloud service provider	Internal organization	mixed	Community or Third party
Control	Less control	Full control	moderate	Less control
Vulnerability	Highly vulnerable	Less vulnerability	Reduce vulnerability	Less vulnerability
Resources	Full Utilization	Underutilization	moderate	Full utilization
Availability	On demand/ pay per usage	Always on	Depends on contract	Depend on usage

From the table above, it can be infer that, though public cloud is cheap and is managed by service provider but the low security it provided is a concern for clients. Meanwhile private cloud is expensive but it provides high security.

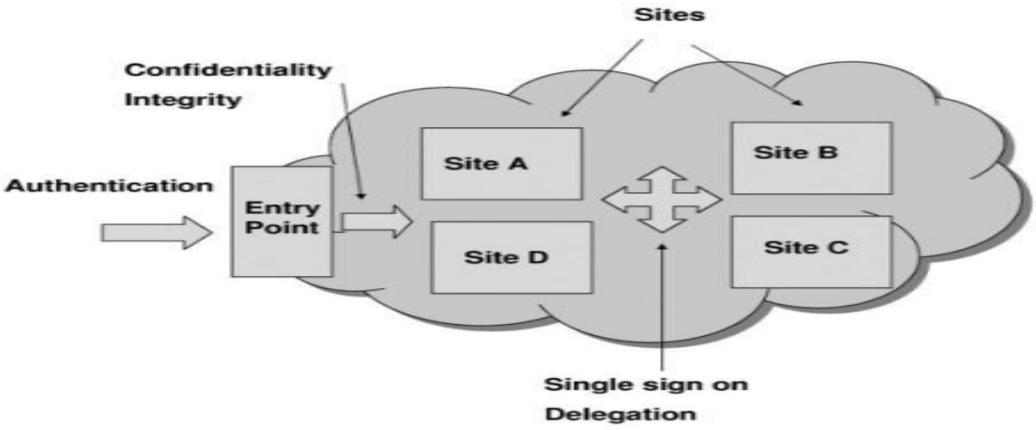


Figure 5: Cloud Computing Security Architecture Design

6. CONCLUSIONS AND RECOMMENDATION

Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Cloud Computing provides an efficient and flexible way for services to meet escalating business needs. Cloud-shared infrastructure and associated services make it cost effective alternative to traditional approaches. Perhaps the biggest concerns about cloud computing are security and privacy. In this paper we present a study of different security issues and challenges that could occur in a cloud environment. We also present as brief overview of cloud service models and also compare them. Few security and challenges that could occur in a cloud environment is given.

REFERENCES

1. C. W. Yoon, M. M. Hassan, H. W. Lee, et. al., ―Dynamic Collaborative Cloud Service Platform: Opportunities and Challenges‖, ETRI Journal, vol. 32, no.4, **(2010)**, pp. 634–637.
2. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., Molina, J.: Controlling Data in the Cloud: Outsourcing Computation Without Outsourcing Control. In Proceedings of the 2009 ACM workshop on Cloud Computing Security, (2009).
3. Imran Ashraf, ‖ An Overview of Service Models of Cloud Computing‖, International Journal of Multidisciplinary and Current Research (2014)
4. J. Gaudiosi, "Future of Cloud Gaming: Industry Leaders' Thoughts", FC Business intelligence, **(2011)**.
5. K. Hwang, G. Fox and J. Dongarra, ―Distributed and Cloud Computing: from Parallel Processing to the Internet of Things‖, Morgan Kauffman Publishers, **(2011)**.
6. Lombardi, F., Di Pietro, R.: Secure virtualization for cloud computing. Journal of Network and Computer Applications, 34(4), (2011).
7. Osama, H., Bader, A., Nazeeh, G., Ruba, O., Mua'ad, A., Hossam, F: Data Security Issues and Challenges in Cloud Computing. A conceptual Analysis and Review. Scientific Research Communication and Network 2014, 6, 15-21. Published Online February 2014
8. wikipedia http://en.wikipedia.org/wiki/Cloud_computing_securit
9. Anand M., Bina B, Security in Cloud Computing - Vulnerabilities, Challenges, Models and path ahead(2012)
10. Sabahi, F.: Secure Virtualization for Cloud Environment Using Hypervisor-based Technology. Int. Journal of Machine Learning and Computing, 2(1), (2012).
11. Sefton, P.: Privacy and Data Control in the Era of Cloud Computing. Brightline Lawyers, (2010).
12. Neela, K. L & .Kavitha, V., 2013: A Survey on Security Issues andVulnerabilities on Cloud ComputingInternational Journal of Computer Science & Engineering Technology ISSN : 2229-3345 Vol. 4 No IJCSEThttp : // cloudcomp uting.sys.con .com.' node.'http : //www.parc.com. contentiattachments.Control ling DatalnTheCloud-CCS W-09.pdf
13. http ://www.cloudcomputing.sys-con.coniinode.‖
14. http: //www.cloudsccurityalliance.org