Journal of Basic and Applied Engineering Research
Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 1, Number 6; October, 2014 pp. 104-107
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/jbaer.html

Analysis of Cloud Computing and Security Challenges

Mohsin Raza

Al-falah University, Faridabad, Haryana, (India)

Abstract: **Cloud computing, a rapidly developing information technology is an internet based computing in which large groups of remote servers are networked so as to allow sharing of data processing tasks, centralized data storage, and online access to computer services or resources. Cloud computing is at an early stage, with a motley crew of providers large and small delivering a slew of cloud-based services, from full-blown applications to storage services to spam filtering. Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet). The main aim of cloud computing is to provide a powerful computing at low cost with higher level of availability with security and privacy. Cloud computing is broadly divided in to three parts – public cloud, private cloud and hybrid cloud. To distribute a powerful computing to end users Cloud services are divided in to three categories – Infrastructure-as-a-Service (IaaS), Platform as a Service (PaaS), Software-as-a-Service (SaaS).**

This paper explains an analysis on cloud computing, its architecture and the type of services available in cloud computing. The security and privacy of data are biggest concern in cloud computing. This paper also highlights the privacy of data and security challenges in cloud computing.

Keywords: **cloud computing, IaaS, PaaS, SaaS, public cloud, private cloud, hybrid cloud, security**

1. INTRODUCTION

Cloud computing is a compilation of existing techniques and technologies, packaged within a new infrastructure paradigm that offers improved scalability, elasticity, business agility, faster startup time, reduced management costs, and just-in-time availability of resources [1]. The cloud computing is not a new concept. This is a new flavor of existing technologies with add on as per new Information technology (IT) industries requirements. Cloud computing has generated a significant interest to researcher and IT industries to enter in a new mode of business computing. The main objective of cloud computing is to provide a solution to IT industries / individuals which will be fast , reliable, secure , available and cost effective. Cloud Computing provides on-demand hardware (like Server), storage resources, services hosting and services management environment, and other devices as a utility or resource over a network, rather than having own local servers or personal devices to handle manage services and applications as given in figure 1.

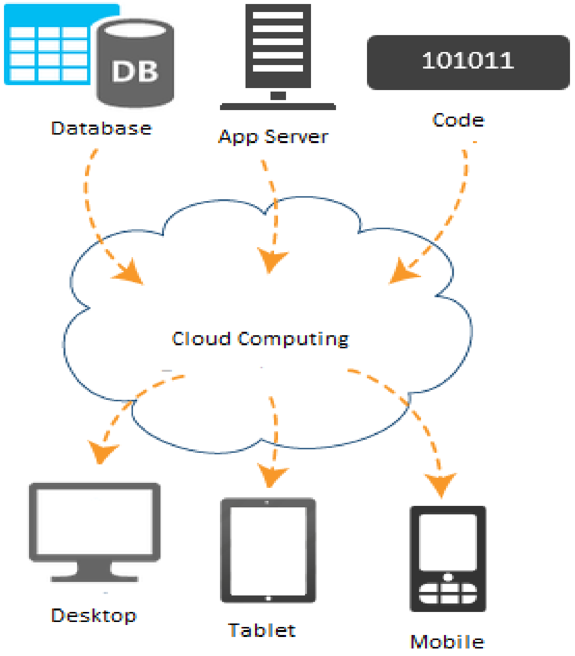

Fig. 1: Cloud computing

Nevertheless, cloud computing is an important paradigm, with the potential to significantly reduce costs through optimization and increased operating and economic efficiencies [2]. Privacy and security of data are two main attributes of cloud computing. A recent survey shows that data security and privacy risks have become the primary concern for people to shift to cloud computing [3].

2. AN OVERVIEW OF CLOUD COMPUTING

“Cloud computing” is the next natural step in the evolution of on-demand information technology services and products. To a large extent, cloud computing will be based on virtualized resources [4]. Cloud Computing is often described as a stack, as a response to the broad range of services built on top of one another under the moniker “Cloud.”

A. Definition

Cloud Computing is a model for enabling 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 [5].

There are several characteristics that it sees as essential for a service to be considered “Cloud.” These characteristics include:

- On-demand self-service. The ability for an end user to sign up and receive services without the long delays that have characterized traditional IT.
- Broad network access. Ability to access the service via standard platforms (desktop, laptop, mobile etc).
- Resource pooling. Resources are pooled across multiple customers [6].
- Rapid elasticity. Capability can scale to cope with demand peaks [7].
- Measured service. Billing is metered and delivered as a utility service [8].

B. Architecture

There are four main components in cloud computing namely cloud structure, cloud storage, cloud platform and cloud services as given in figure 2.

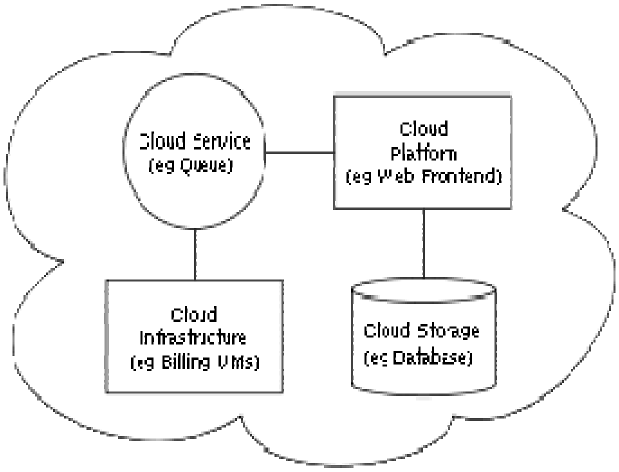
Cloud Service (eg Queue)
Cloud Platform (eg Web Frontend)
Cloud Infrastructure (eg Billing VMs)
Cloud Storage (eg Database)

Fig. 2: Architecture of cloud computing

B. Deployment Model

Based on the end user’s requirements, a cloud infrastructure may be operated in the following three type of deployment model: public cloud, private cloud and hybrid cloud.

Public cloud: A public cloud is one in which the cloud services are open to the general public over a public network. A public cloud services may be free or offered on a pay-per-usage model. A public cloud is maintained by an organization selling cloud services and serves a diverse pool of clients [9]. A simple view of public cloud with its customers is given in below figure 3.

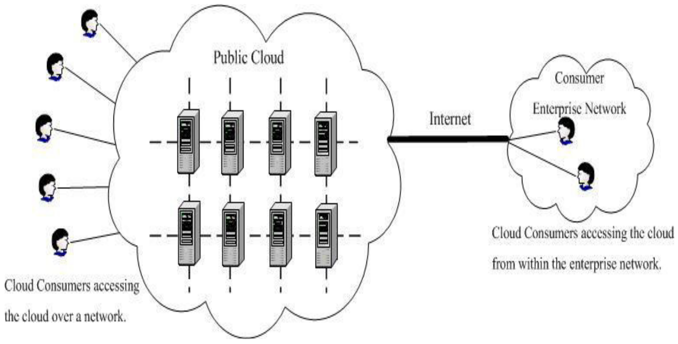
Public Cloud
Internet
Consumer Enterprise Network
Cloud Consumers accessing the cloud from within the enterprise network.
Cloud Consumers accessing the cloud over a network.

Fig. 3: Simple public cloud deployment model

Private cloud: Private cloud is cloud infrastructure in which a single cloud consumer’s organization exclusive access to and usage cloud services and computational resources. Private cloud infrastructure may be managed either by the cloud consumer organization or by a third party, and may be hosted on the organization’s premises or outsourced to a hosting company. A private cloud model is given in figure 4.

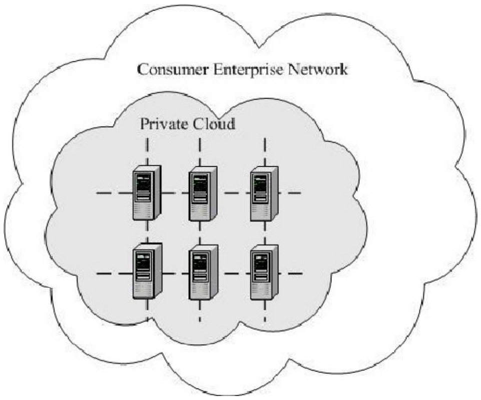

Fig. 4: Private cloud model

Hybrid Model: Hybrid cloud is a composition of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models [10].

Service Models

The service model is categorized in to three models as Service- as - Software-as-a-Service (SaaS), Platform–as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) as given in figure 5.

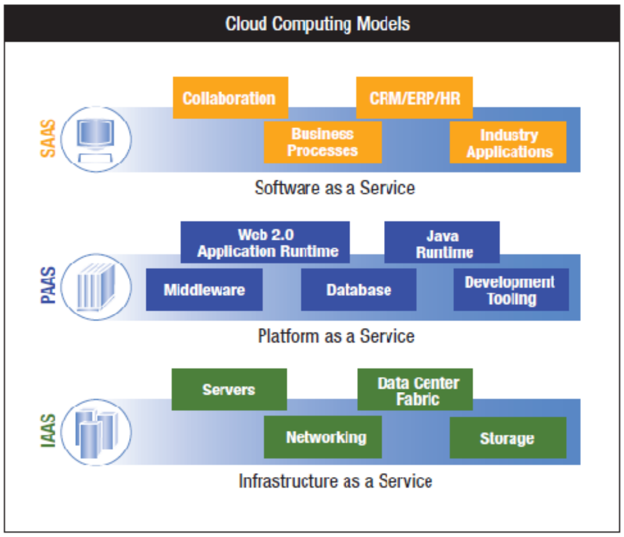

Fig. 5: Service models of cloud computing.

Software-as-a-Service (SaaS)*:* SaaS is a software that is designed for end users and delivered over the web/internet. With SaaS, a service provider licenses an application/software as a service on demand in a pay-as-you-go model. This type of service model delivers a single application through the browser to thousands of customers using a multitenant architecture. Salesforce.com is a best-known example among enterprise applications [11].

Platform–as-a-Service (PaaS): PaaS is the set of tools and services designed to make coding and deploying those applications quick and efficient. PaaS is another type SaaS which provide development environment as a service. The best example of PaaS is to use of third party algorithm in own program and deliver it to the end users through web/internet.

Infrastructure-as-a-Service (IaaS): IaaS is a way of delivering Cloud Computing infrastructure – servers, storage, network and operating systems – as an on-demand service. Rather than purchasing servers, software, datacenter space or network equipment, clients instead buy those resources as a fully outsourced service on demand

3. CHALLENGES IN CLOUD COMPUTING

Cloud computing encompasses activities such as the use of social networking sites and other forms of interpersonal computing; however, most of the time cloud computing is concerned with accessing online software applications, data storage and processing power. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is [12]. In this section we focus the challenges or hurdle of cloud computing with associated security issues.

A. Security

Security is the biggest concern to organization who are being the users of cloud computing. In cloud computing the data will be distributed over the individual computers and the software is running on some ones else hard disk. Data loss, phishing, botnet (running remotely on a collection of machines) is the serious threats to the organization's data and software. Moreover, the multi-tenancy model and the pooled computing resources in cloud computing has introduced new security challenges that require novel techniques to tackle with. For example, hackers can use Cloud to organize botnet as Cloud often provides more reliable infrastructure services at a relatively cheaper price for them to start an attack [13].

B. Trust

Trust revolves around 'assurance' and confidence that people, data, entities, information or processes will function or behave in expected ways. Trust may be human to human, machine to machine (e.g., handshake protocols negotiated within certain protocols), human to machine (e.g., when a consumer reviews a digital signature advisory notice on a web site) or machine to human (e.g., when a system relies on user input and instructions without extensive verification). At a deeper level, trust might be regarded as a consequence of progress towards security or privacy objectives.

C. Privacy

The cloud is like a black box, nothing inside the cloud is visible to the clients. The data in the cloud are easier to manipulate and there may be high chances that malicious programs violate the confidentiality and integrity of the data. Privacy concerns the expression of or adherence to various legal and non legal norms. The cloud providers must implement panoply to secure privacy and protection of personal data.

D. Regulatory compliance

Compliance touches on many issues, depending on the industry and requirements of the customer. Compliance is an issue that, along with security and privacy, often inhibits the adoption of cloud computing. In many cases, however, these issues can be addressed with a combination of contract provisions, careful vetting of vendors, the adoption of granular security procedures and, to some extent, insurance protections. Companies should consult counsel that is familiar with the specific regulatory requirements of the business.

Customers need to address and understand, in the contract with the cloud provider, what happens when they must respond to legal discovery or a regulatory subpoena. Like the horizontal interoperability issue, the format for the extracted data, the length of time needed to extract the data, the vendor's ability to search and cull the data and the cost of extraction are all important issues.

E. Reliability

The service level agreement (SLA) should cover reliability. Availability, bandwidth and vertical interoperability should be addressed with as much specificity as necessary. A guarantee of 99 percent availability actually means that the service could be out for an entire day every 100 days. Many availability provisions do not address throughput or bandwidth. The service could be up, but unacceptably slow, and still be considered "available" under the contract. Customers should also understand that there may be exceptions in the contract that do not count towards the availability or related guarantees, such as the service being down for maintenance as the result of events outside of the vendor's control. This is not to say that cloud vendors should be expected to guarantee 100 percent availability or ideal throughput all of the time, but only that both parties should understand and properly document their expectations

F. Complexity

Complexity is a subset of interoperability and intersects with other issues such as regulatory compliance. It is often addressed through careful planning and in a meaningful and granular implementation and testing process. Like enterprise resource planning projects, cloud computing projects require a detailed understanding of the customer's workflows and the scope of work. Customers should beware of vendors promising that "we can do that" if the vendor does not take the time to understand the client's business needs. All too often, the sales promises turn into vague scope-of-work requirements in the SLA and problems during the testing and implementation phases. On the vendor's side, the customer's failure to commit the resources necessary to implement the project may also create problems. Spending time on all of these issues at the beginning of the relationship and incorporating the understandings into the contract gives the project a better chance at success.

4. CONCLUSION

Cloud computing is an emerging technology in Information Technology (IT) which cannot be described in single entity rather than providing the means through which everything - Infrastructure as a Service at the base, through Platform as a Service as a development tool and through to Software as a Service replacing on-premise applications. In this paper we analysis the definition of cloud computing with various scenario, describe the deployment models, explain the service model and focus the issues of cloud computing with security as a prime concern. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.

REFERENCES

[1] Naval Research Lab "Security Issues in Cloud Computing"

[2] D. Catteddu and G. Hogben, "Cloud Computing: Benefits, Risks and Recommendations for Information Security,"

[3] Randolph Barr, qualys Inc, "How to gain comfort in losing control to the cloud"

[4] Mladen A. Vouk, "Cloud Computing – Issues,Research and Implementations"

[5] http://csrc.nist.gov/groups/SNS/cloud-computing/

[6] Virtualization – The ability to increase computing efficiency http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Revolution_Not_Evolution-Whitepaper

[7] Scalability and fast provisioning – for IT at web scale – http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Revolution_Not_Evolution-Whitepaper.pdf

[8] From Water-wheel to Utility Power – An analogy for the Cloud-http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Revolution_Not_Evolution-Whitepaper.pdf

[9] Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf, "NIST Cloud computing reference architecture"

[10] http://en.wikipedia.org/wiki/Cloud_computing.

[11] http://www.qrimp.com/blog/blog.The-Difference-between-IaaS-and-PaaS.html

[12] Jianfeng Yang, Zhibin Chen, "Cloud Computing Research and Security Issues"

[13] S. Ramgovind, M. M. Eloff, E. Smith. "The Management of Security in Cloud Computing" In PROC 2010 IEEE International Conference on Cloud Computing 2010.