International Journal of Future Generation Communication and Networking
Vol. 13, No. 3, (2020), pp. 1415–1423

Cloud Computing Environment: Benefits and Challenges

[1]*Uma Hombal*
[1]*Research Scholar, Department of Computer Science, KSIT Bangalore*
uhombal@gmail.com

Abstract

Cloud computing has emerged as a new paradigm in computation as well as hosting and delivering services over the internet. During the past few years, cloud computing has become a key IT buzzword. It is an emerging model of business computing. Cloud computing has transformed the way information technology (IT) is consumed and managed, promising improved cost efficiencies, accelerated innovation, faster time-to-market, and the ability to scale applications on demand (Leighton, 2009). It promises reliability, scalability, and decreased costs, which have attracted businesses, enterprises, and individuals.Many Companies that are considered to be giants in software industry like Google, Facebook, Amazon, Microsoft, Yahoo and many more are joining to develop Cloud services. Even though there are numerous advantages of cloud computing, it also introduces a series of security concerns. However we identified several challenges from the cloud computing adoption perspective. We explore the concept of cloud architecture and identify and relate vulnerabilities and threats related to cloud computing. This paper focuses on understanding the different issues and concerns in adopting cloud as it is a fundamental requirement before enjoying the benefits of cloud.

I. INTRODUCTION

Cloud computing has emerged as a new paradigm in computation as well as hosting and delivering services over the internet. The cloud computing is an internet-based environment that allows us to use software, data, and services over the internet from any location on any web enabled device [1]. The definition of "cloud computing" from the National Institute of Standards and Technology (NIST) [2] is that cloud computing enables 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. According to this definition, it provides a convenient on-demand network access to a shared pool of computing resources such as computing applications, network resources, platforms, software services, virtual servers, computing infrastructure, etc. Cloud computing provides on-demand services at a very minimal cost. It delivers computing resources over the Internet whereby individuals and businesses can use software and hardware managed by third parties at remote locations. Cloud-computing platform also provides on- demand services, anywhere, anytime. The importance of Cloud Computing is increasing and it is receiving a greater attention in both scientific and industrial communities. Cloud Computing appears as a computational paradigm as well as a distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet [3,4]. The cloud enhances collaboration, agility, scalability, availability, ability to adapt to fluctuations according to demand, accelerate development work, and provides potential for cost reduction through optimized and efficient computing [5-8]. Cloud Computing combines a number of computing concepts and technologies such as Service Oriented Architecture (SOA), Web 2.0, virtualization and other technologies with reliance on the Internet, providing common business applications online through webbrowsers to satisfy the computing needs of users, while their software and data are stored on the servers[6]. Insome respects, Cloud Computing represents the maturingof these technologies and is a marketing term torepresent that maturity and the services they provide [7].Although there are many benefits to adopting CloudComputing, there are also

ISSN: 2233-7857 IJFGCN

some significant barriers toadoption. One of the most significant barriers to adoptionis security, followed by issues regarding compliance, privacy and legal matters [9].

II Essential Characteristics of Cloud Computing

National Institute of Standards and Technology (NIST) defined five characteristics of cloud computing (CC). Essential characteristics include:

1) Broad Network Access and Shared Infrastructure

Cloud computing provides access to capabilities over the network through thin or thick client platform (for example, mobile phone, laptops, and others) through some standard mechanisms.Cloud providers invest in and build the infrastructure necessary to offer software, platforms or infrastructure as a service to multiple consumers. Capabilities are available through shared networks with multitenant customers. Provider's resources are pooled to serve multiple consumers using multitenant model. The user can access the data of the cloud or upload the data to the cloud from anywhere just with the help of a device and an internet connection. These capabilities are available all over the network and accessed with the help of internet.Because of the need to leverage the infrastructure across many consumers, cloud vendors need create a more agile and efficient infrastructure that can move consumer workloads, minimize overheads and increase service quality.

2) On-Demand Self-Service

It is one of the important and valuable characteristics of cloud computing as the customers will be able to purchase and use the services of cloud as and when there is need. In some of the cases, cloud vendors provide an Application Programming Interface (API) which helps the customer to automatically consume a service and can also monitor the computing capabilities.The Cloud computing services does not require any human administrators. The customers themselves are able to provision, monitor and manage computing resources as needed.

3) Elasticity and Scalability

Traditionally on-premises architectures can't scale as easily. The enterprises have to plan for peak capacity and have those extra resources sit idle during less activity, which can rack up costs. From the customer viewpoint, it is the ability to expand and reduce resources according to their specific requirement. This capability provides an elastic and scalable IT resource. Consumers pay for only the services they use. Although no IT service is infinitely scalable, the cloud service provider's ability to meet the consumer's IT needs creates the perception that the service is infinitely scalable and increases its value. Resource pooling enables scalability for cloud providers and users because compute, storage and networking assets can be added or removed as needed. This helps enterprise IT teams to optimize their cloud-hosted workloads and avoid end-user bottlenecks.

4) **Measured Services**

Cloud computing automatically controls and optimizes resource usage by leveraging a metering capacity at some level of abstraction which is appropriate to the type of service. Cloud frameworks automatically control and upgrade the cloud resource use by utilizing a metering ability at the level of abstraction suitable to the kind of administration (e.g., stockpiling, planning, exchange speed and dynamic customer accounts). Resource usageis observed, controlled and revealed, giving straightforwardness and clear picture to the supplier and customer. The resource utilization is tracked for each application and occupant, it will provide both the user and the resource provider with an account of what has been used. This is done for various reasons like monitoring billing and effective use of resource. This resource utilization is analyzed by supporting charge-per-use capabilities, which means that the resource usages that are running in the cloud are getting monitored, measured and reported by the service provider.

ISSN: 2233-7857 IJFGCN

5) **Multi-tenancy**
In a private cloud, the customers are also called tenants, can have different business divisions inside the same company. In a public cloud, the customers are often entirely different organizations.

Most public cloud providers use the multi-tenancy model. Multi-tenancy allows customers to run one server instance, which is less expensive and makes it easier to deploy updates to a large number of customers.

6) **Resiliency**

Cloud providers use a number of techniques to guard against downtime, such as minimizing regional dependencies to avoid single points of failure. Users can also extend their workloads across availability zones, which have redundant networks connecting multiple data centers in relatively close proximity. Some higher-level services automatically distribute workloads across availability zones. Outages occur and enterprises must have contingency plans in place. For some, that means extending workloads across isolated regions or even different platforms, though that can come with a hefty price tag and increased complexity.
7) **Availability**
The capabilities of the cloud can be modified as and when needed and can be extend a lot. It analyzes the storage usage and allows the user to buy extra cloud storage if need be for a very small amount. This service is available anytime and can be accessed from anywhere.

III CLOUD COMPUTING MODELS

There are four basic cloud delivery models, as outlined by NIST, based on who provides the cloud services. There are four primary ways in which cloudservices are deployed (CSA Security Guidance, 2009).

1) Public Cloud

It is a type of cloud hosting in which the cloud services are delivered over a network that is open for public usage. This model is true representation of cloud hosting. Public clouds are provided by a designated service provider and offer either a single tenant (dedicated) or multi-tenant (shared) operating environment with all the benefits and functionality of elasticity and the accountability/utility model of cloud. The physical infrastructure is generally owned by and managed by the designated service provider and located within the provider's data centers (off premises). Customers do not have any control over the location of the infrastructure. Public cloud is suited for business which require managing load. All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. Due to the decreasing capital overheads and operational cost, the public cloud model is economical. One of the advantages of a public cloud is that they may be largerthan an enterprise cloud, and hence they provide the ability to scale seamlessly on demand.

2) Private Cloud

It is also known as internal cloud. Private clouds are provided by an organization or their designated services and offer a single-tenant (dedicated) operating environment with all the benefits and functionality of elasticity and accountability/utility model of cloud. The private clouds aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud. Private cloud permits only the authorized users and gives the organization greater control over their data. The physical computers may be hosted internally or externally. Businesses having unanticipated or dynamic needs, assignments which are critical management demands and uptime requirements are better suited to adopt private cloud. In private cloud there is no need for additional security regulations and bandwidth limitations that can be

ISSN: 2233-7857 IJFGCN

present in a public cloud environment. Clients and Cloud providers have control of the infrastructure and improved security, since user's access and the networks used are restricted.

3) Hybrid Cloud

It is a type of cloud computing, which is integrated. It is an adaptation between two platforms in which the workload is exchanged between the private cloud and the public cloud as per the user's needs and demand of organization. Resources which are non-critical like development and test workloads can be housed in the public cloud that belongs to a third-party provider. While the workloads that are critical or sensitive should be housed internally. It allows the user to increase the capacity as well as the capability by assimilation, aggregation and customization with another cloud package / service. The hybrid cloud model is capable of providing on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload.

4) Community Cloud

It is a type of cloud hosting in which the setup is mutually shared between a lot of organizations which belong to a particular community like banks and business firms. It is a multi-tenant setup that is shared among many organizations that belong to a group which has similar computing apprehensions. These community members usually share similar performance and security concerns. The main intention of the communities is to achieve business related objectives. Community cloud can be managed internally or can be managed by third party providers and hosted externally or internally. The cost is shared by specific organizations within the community, therefore, community cloud has cost saving capacity. Organizations have realized that cloud hosting has a lot of potential. To be the best one must select the right type of cloud hosting Therefore, one need to know the business and analyze his/her demands. Once the appropriate type of cloud hosting is selected, one can achieve business related goals easily.

IV Cloud computing service models

The service models are categorized into three basic models[10]:

1) Software-as-a-Service (SaaS)
2) Platform-as-a-Service (PaaS)
3) Infrastructure-as-a-Service (IaaS)

ISSN: 2233-7857 IJFGCN

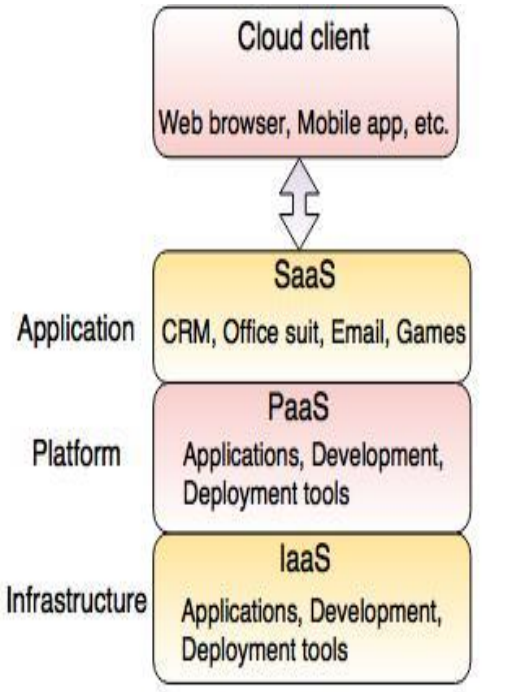

Fig. - Categories of Cloud Computing

Software-as-a-Service (SaaS)

SaaS is known as **'On-Demand Software'.**It is a software distribution model. In this model, the applications are hosted by a cloud service provider and publicized to the customers over internet.SaaS makes uses the web to provide applications which are managed by a third-party vendor and whose interface is accessed on the client side. SaaS applications can be run from a web browser without the need to download or installation, but these require plugins.In SaaS, associated data and software are hosted centrally on the cloud server.User can access SaaS by using a thin client through a web browser.CRM, Office Suite, Email, games, etc. are the software applications which are provided as a service through Internet.The companies like Google, Microsoft provide their applications as a service to the end users.The key benefit of SaaS is that it requires no advance investment in servers or licensing of software. The application developer has to maintain one application for multiple clients.

3.1: Software as a Service (SaaS)

The cloud provider provides the consumer with the ability to deploy an application on a cloud infrastructure [5].Because of this web delivery model SaaS removes the need to install and run applications on individual computers. In this model it is easy for enterprises to improve their maintenance and support, because everything can be managed by vendors: applications, runtime, data, middleware, OS, virtualization, servers, storage and networking. Popular SaaS services include email and collaboration, healthcare-related application. SaaS providers usually offer browser-based interfaces. APIs are also normally made available for developers. The key benefit of SaaS is that it requires no advance investment in servers or licensing of software. The application developer, have to maintain one application for multiple clients. In summary, in this model, the customers do not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Currently, SaaS is offered by companies such as Google, Salesforce, Microsoft, Zoho etc.

ISSN: 2233-7857 IJFGCN

Infrastructure as a Service (IaaS)

IaaS is a way to deliver a cloud computing infrastructure like server, storage, network and operating system.The customers can access these resources over cloud computing platform i.e Internet as an on-demand service. In IaaS, you buy complete resources rather than purchasing server, software, datacenter space or network equipment.Users can purchase IaaS based on consumption, similar to other utility billing. IaaS users have the responsibility to be in charge of applications, data, runtime and middleware. Providers can still manage virtualization, servers, storage, and networking. The customerhas the freedom to build his own applications, which run on the provider's infrastructure. Hence, acapability is provided to the customer to deploy onto the cloud infrastructure customer-createdapplications using programming languages and tools supported by the provider (e.g., Java, Python, .Net etc.). Although the customer does not manage or control the underlying cloud infrastructure, network,servers, operating systems, or storage, but he/she has the control over the deployed applications andpossibly over the application hosting environment configurations. To meet manageability and scalabilityrequirements of the applications, PaaS providers offer a predefined combination of operating systems andapplication servers, such as LAMP (Linux, Apache, MySql and PHP) platform, restricted J2EE, Ruby etc.Some examples of PaaS are: Google's App Engine, Force.com, etc.

PaaS (Platform as a Service)

PaaS is a programming platform for developers.Platform as a service (PaaS) is a kind of cloud computing services that provides a platform that allows customers to develop, run, and manage applications without the problem of building and maintaining the infrastructure. One need not be bothered about lower level elements of Infrastructure, Network Topology, Security all this is done for you by the Cloud Service Provider. PaaS gives the runtime environment for application development and deployment tools.A developer can easily write the application and deploy it directly into PaaS layer.A PaaS cloud provides useful software building blocks, and a number of development tools that assist in deploying new applications. Google Apps Engine(GAE), Windows Azure, SalesForce.com are the examples of PaaS.

Challenges of cloud computing

Cloud computing is very promising for the IT applications; however, there are still some problems to be solved for personal users and enterprises to store data and deploy applications in the cloud computing environment. Despite the potential benefits of cloud computing, the organizations are slow in accepting it due to the following limitations: data loss, data cleaning, account hijacking, less control over the process, insider attacks by the CSP's, lack of legal aspects, lack of portability/migration from one service provider to another, less reliable, lack of auditability, less QoS. These limitations lead to the issues or challenges such as – security, interoperability, virtualization, data leakage, resource sharing, load balancing, multi-tenancy, and Service Level Agreement (SLA). Some of the Challenges of Cloud Computing are

1. Outsourcing Data and Applications: Cloud user deploys data and applications on cloud servers by depending on third parties to make decisions about user data and platforms. Cloud Computing provides access to data, but the biggest challenge is to ensure that only authorized user can gain access to it (Takabi et al., 2010). It is very difficult to have appropriate mechanisms to prevent cloud providers from using customers' data in a way that has not been agreed upon.

2. SLA (Service Level Agreement): It is essential for customers to get assurances from providers on service delivery. Typically, these are provided during SLAs negotiated between the providers and customers (John et al., 2009). It is difficult to define SLA specification and different cloud offerings will need to classify different specifications.

ISSN: 2233-7857 IJFGCN

3. Extensibility and Shared Responsibility: Cloud providers and customers must share the responsibility for security and privacy in cloud computing environments, but sharing levels will differ for different delivery models, which in turn affect cloud extensibility (Takabi et al., 2010). The difficulty lies in providing privacy and security to all deployment models and private clouds could also demand more extensibility so as to accommodate customized requirements and so providing security at that stage could be difficult.

4. Cloud Interoperability: Which provide the freedom to customer to switch from alternative vendors/offerings/providers simultaneously to optimise resources at various stages in an organization(Gundeep et al., 2012). Cloud APIs makes it very difficult to merge cloud services with an organisation's own existing legacy systems. The main objective of interoperability is to detect the faultless fluid data across local applications, across clouds and among clouds and it is difficult to detect.

5. Heterogeneity: Cloud providers use various hardware and software resources to build cloud environments. To some extent, resource virtualization achieves high level system homogeneity, but the same infrastructure being used to support different tenants with different protection and system requirements can generate difficulties (Takabi et al., 2010). Difficulties here could be if a client subscribes to different cloud providers for different services then the assumptions that each of these cloud providers make in building the services can severely affect the emergent trust and security properties. It also generates integration challenges. Also in a multi-tenant environment, the protection requirements for each tenant might differ, which can make a multi-tenant cloud a single point of compromise.

6. Multi-tenancy: This means that the cloud platform is shared and exploited by number of clients (Bhaskar et al., 2009; Xiao and Xiao, 2012). One of the difficulty is opponents who may also be legal cloud clients may utilize the co-residence issue. Many security issues such as data breach, computation breach, flooding attack, etc., are incurred. It supplies new vulnerabilities to the cloud platform.

7. Load Balancing: Load balancing can be defined as assigning a part of job to another or idle computer to improve the efficiency and optimize the use of resources (Tsai et al., 2010). Continuous monitoring of the components becomes overhead and when one becomes non-responsive, the load balancer needs to inform that stop sending traffic to overloaded system.

8. *Resource scheduling:* Means assigning the resources such as hardware, software, process time, communication bandwidth and applications tothe processes. Implementing multitasking and multiplexing techniques in scheduler is somewhat tedious task.

9. *Virtualisation:* IT virtualisation is the abstraction of physical infrastructures such as servers, data centres, networks capabilities and storage resources (Tsai et al., 2010). Rise of high density is one of the difficulty and reduced IT load affects power usage effectiveness (PUE).

10. *Privacy and security:* A third party causes the security and privacy issuesmore critical when outsourcing the data and business applications (Bhaskar et al.,2009). Finding the solutions for the attacks Malware-injection, flooding, accountability check problem, browser security, securing data in transmission, identity and access management is difficult.

ISSN: 2233-7857 IJFGCN

CONCLUSION

Cloud computing technology is the emerging technology whichprovide the facilities of software and hardware over internet on demand.The cloud computing provides convenient on-demand access of the data[12]. A less expensive technology to share the resource over internet. It isa technology that is based on internet. But it also raises some security problems which may affect its usage. Understanding about the vulnerabilities existing in Cloud Computing will help organizations to make the shift towards using the Cloud. Since Cloud Computing leverages many technologies and it also inherits their security issues, traditional web applications, virtualizations have been looked over but some of the solutions offered by cloud are immature or inexistent. This paper reviewed cloud computing paradigm from various perspectives such as concepts, cloud platforms, three service models, deployment models and challenges. Various general challenges of cloud computing and the number of difficulties involved in those challenges are identified. The possible solutions would help the researchers to have proper directions for future research and to get into the efficient implementation of the techniques.

REFERENCES:

[1]K. B. Deepaklal, "Fuzzy Keywoard Search over Encrypted Data in Multicloud", Discovery, Volume 3, Issue 1, January – February 2014.

[2] P.Mell and T. Grance, "The nist definition of cloud computing,"National Institute of Standards and Technology, vol. 53, no. 6,article 50, 2009

3. Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N (2009) CloudComputing: A Statistics Aspect of Users. In: First International Conference onCloud Computing (CloudCom), Beijing, China. Springer Berlin, Heidelberg,pp 347–358

4. Zhang S, Zhang S, Chen X, Huo X (2010) Cloud Computing Research and Development Trend. In: Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China. IEEE Computer Society, Washington, DC, USA, pp 93–97

5. Cloud Security Alliance (2011) Security guidance for critical areas of focus in Cloud Computing V3.0.. Available: https://cloudsecurityalliance.org/ guidance/csaguide.v3.0.pdf

6. Marinos A, Briscoe G (2009) Community Cloud Computing. In: 1st International Conference on Cloud Computing (CloudCom), Beijing, China. Springer-Verlag Berlin, Heidelberg

7. Centre for the Protection of National Infrastructure (2010) Information Security Briefing 01/2010 Cloud Computing. Available: http://www.cpni.gov. uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf

8. Khalid A (2010) Cloud Computing: applying issues in Small Business. In: International Conference on Signal Acquisition and Processing (ICSAP'10),pp 278–281

9. KPMG (2010) From hype to future: KPMG's 2010 Cloud Computing survey.. Available: http://www.techrepublic.com/whitepapers/from-hype-to-futurekpmgs- 2010-cloud-computing-survey/2384291

10. https://www.tutorialride.com/cloud-computing/service-models-in-cloud-computing.htm

ISSN: 2233-7857 IJFGCN

[11]. H. Takabi, J.B.D. Joshi, and G.-J. Ahn, "Secure Cloud: 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.

12 Uma Hombal, Dr. Dayananda R. B, "Secure and Optimized Data Sharing Model Group in Healthcare Cloud Environment", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-1, November 2019

ISSN: 2233-7857 IJFGCN