International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 4228–4237

CLOUD COMPUTING: ARCHITECTURE AND CHALLENGES

K. SRINIVASA RAO*1, B. DIVYA REKHA*2, K. MOUNICA*3
1. Lecturer In Computer Science, Bhavan's Vivekananda College,
Sainikpuri, Secunderabad, Telangana, India
ksrbhavans@gmail.com

2. Lecturer In Computer Science, Bhavan's Vivekananda College,
Sainikpuri, Secunderabad, Telangana, India
B.D.Rekha@gmail.com

3. B.Tech (ECE), Geethanjali College of Engineering and Technology,
Cheeryal [V], Keesara [M], Hyderabad, Telangana, India
kakarlamounica96@gmail.com

Abstract

Not long ago, cloud computing appeared to be altering Information technology proceedings and also the IT industry. The journey came a long way from the perception of computing in a parallel environment to moving into a distributed computing environment and then proceeded to grid computing and very recently proceeded to cloud computing. Cloud computing serves us in storing and accessing the databases, softwares and analytics that are hosted on the internet instead of computer's local server. It rapidly remodeled in IT as a usage based payment service which facilitates the usage of accessing applications, infrastructure and resources to the consumers as per their requirement provided by cloud contributors The architecture of cloud computing consists of many cloud components which can be majorly classified into front-end and back-end that are connected over a network usually internet. The cloud provides users with three different platforms-SaaS, PaaS and IaaS which can be implemented on any type of deployment model such as public, private, community and hybrid clouds. This paper also presents the various challenges encountered in employing the cloud model.

Keywords*: Introduction, Architecture, Service models, Deployment and Challenges*

1.0 THE EVOLUTION AND THE SCOPE OF CLOUD COMPUTING

The term "cloud" originated from the arena of telecommunications while vendors commenced the Virtual Private Network (VPN) usage for the communication of facts. The following decades saw many technical advancements required for the true cloud computing. The very first operating system called as the Virtual Machine (VM) was introduced by the software giant IBM in 1972.In 1990s several telecommunication companies offered their own versions of VPNs. Cloud computing which thus started caught on rapidly and kept booming.

The National Institute of Standards and Technology [NIST] declared that "Cloud computing is a model for enabling the convenient, on-demand network access to a shared pool of configurable computing resources (ex: Networks, Servers etc) that may be quickly equipped and launched with minimum control attempt or cloud service supplier issuer interaction [1].

ISSN: 2233-7857 IJFGCN

Cloud computing provides with virtualization over a broad network access, rapid elasticity, scalability and inter-operability. In 1966 the qualities of cloud computing have been explored by Douglas Parkhill in his book, The Challenge of the Computer Utility [2].

Scope*:* Cloud supports the business organizations to specialize in their core construct instead of substructure and utility services and also its network helps in plummeting prices of IT Infrastructure. It collectively helps the IT world in the adjustment of the resources during the impulsive and fluctuating demand. The cloud network provides high capability networks, cheap resources, storage devices and service-oriented design. It distributes computing services like storage, servers, networking, databases, software package and analytics through the internet.

2.0 CLOUD COMPUTING ARCHITECTURE

Also known as "layered computing model [3]", this architecture is classified into 4 levels which are as follows.

- Hardware layer
- Infrastructure layer
- Platform layer and
- Application layer

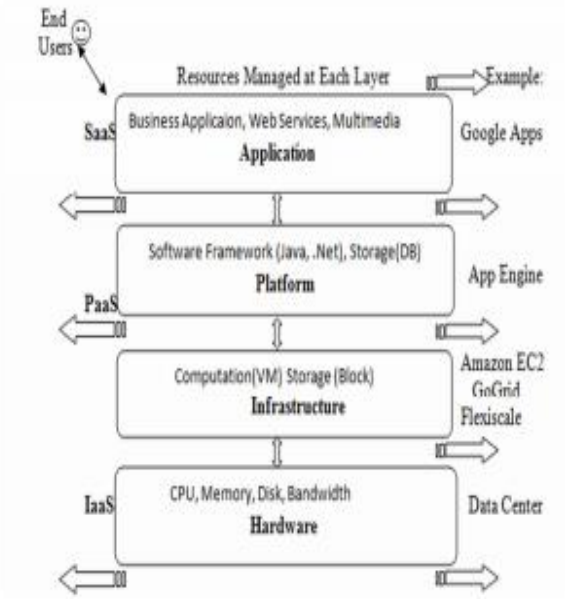


Fig: Cloud computing layered architecture

2.1 Hardware layer:

Hardware layer is also termed as the *physical layer* since this layer consists of all the computer hardware. The whole system runs on the power that is managed at this level. Network connectivity components such as switches, routers can be operated. All these operations occur within the data centre of the cloud. Hardware layer deals with issues such as hardware collapses, resources regulation, traffic management and fault tolerance.

2.2 Infrastructure layer:

Infrastructure layer consists of the servers needed for the virtualization along with several other storage equipment and networking components. It ensures that the resources are

ISSN: 2233-7857 IJFGCN

allocated dynamically to the end users through virtualization technology. It points to the services delivery in the format of host. Through virtualization, the consumers can enjoy the access to the scalable storage and the VM power whenever necessary. It is also responsible for the separation of physical resources.
E.g.: Flexiscale, Amazon EC2.

2.3 Platform layer:

This layer primarily is made of the application framework and the operating system. It is responsible for providing resources to build the applications. It facilitates the end users not only to develop but also test, run and host the applications. All the integrations and the software can be added to the cloud in this layer.
E.g.: Microsoft Azure and GoogleAppEngine.

2.4 Application layer:

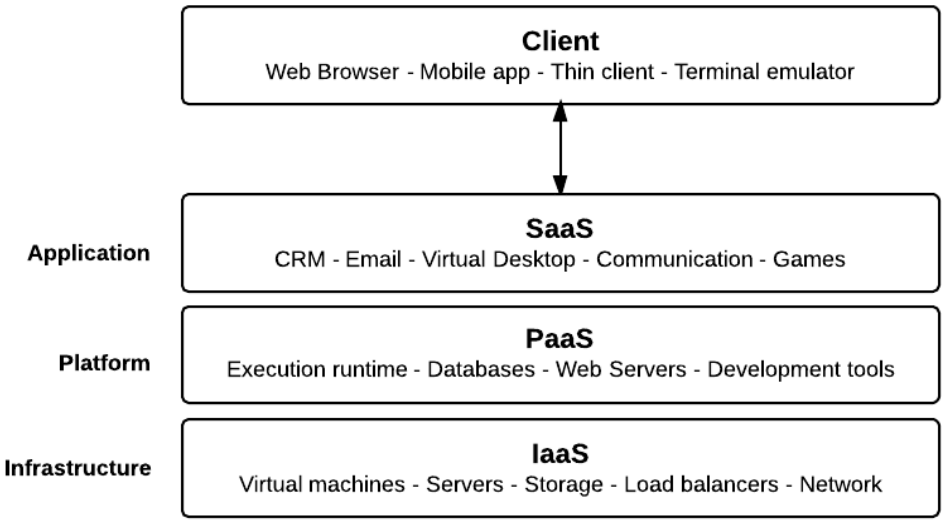
Topmost layer in the cloud topology, this layer deals with the development and the deployment of the several applications which are responsible for the smooth functioning of the cloud by dispensing the right software delivered as service. The entire authentic cloud application is available in this layer which is responsible for essential characteristics such as minimal operational expense, superior execution, scalability and availability. Consumers can easily configure the software systems using metadata. E.g.: Dropbox, Gmail

3.0 SERVICE MODELS OF CLOUD COMPUTING

Cloud computing providers avail their "services" to the users in three different variants. The cloud computing is made available in 3 different service models which can be chosen to satisfy a set of business needs accordingly.

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

The service models are depicted as a layered architecture with each and every layer operating independently.



ISSN: 2233-7857 IJFGCN

Fig: Cloud Delivery-Models

3.1. Infrastructure as a Service (IaaS)

IaaS, also known as Hardware as a Service (HaaS) delivers the computer infrastructure to service various operations on an outsourced basis.

The potential provided to the users is to provide storage, networks, processing and other core computing resources where the consumer can deploy and execute the random software that includes applications as well as the operating systems. The user has no authority to manage or control the underlying essential cloud infrastructure but can control deployed application, storage, operating systems; and perhaps partially be in command of select networking constituents (e.g., host firewalls).

IaaS services avoid capacity planning, obtaining, installation and configuration thereby reducing the time and the expenses in deploying a system [5]. The elevated authorization and its vast chances of configuration guided few researchers to separate this layer into sub layers associated to the resources they depend on (a) data storage, (b) computational resources and (c) communications [7]. IaaS services are widely used for system management, networking and security services. In brief words, IaaS facilitates it's consumers with "MIGRATE" services.

Examples include Azure Stack and Express Route.

3.2 (PaaS) Platform as a Service

PaaS is a cloud computing category that provides a platform and environment to allow developers as well as testers to support debugging, development and install final applications and other services over the internet. PaaS providers host their services on their cloud and infrastructure and are available for the cloud consumers through their web browser. Majority of PaaS contributors dead bolt developers into their software development platforms and prevent direct communication with underlying computing frameworks or supply APIs with limited functionalities [7]. PaaS services are widely used for application development and streaming services. In brief words, PaaS facilitates it's consumers with "BUILD ON IT" services.

Examples: Internet of Things(IoT) and Azure.

3.3. (SaaS) Software as a Service

SaaS is a method of delivering applications and services over the Internet. Alternative to installation and maintenance of the software, users can access the services through the Internet, thereby avoiding the difficult hardware and software management. SaaS billing primarily relies on the features such as usage time, amount of data stored, number of users and number of transactions processed.

This approach banishes the necessity of installation and running the applications on the consumers computers and removes the expenditure on software by on-demand pricing [9].The end users do not have the facility to control the sub lying cloud infrastructure and provides with a possible exception of user-specific configuration settings [4]. SaaS services

ISSN: 2233-7857 IJFGCN

are widely used for ERP, Email, CRM, Collaborative services. In brief words, SaaS facilitates it's consumers with "CONSUME" services.
Examples include SalesForce and GoogleDocs.

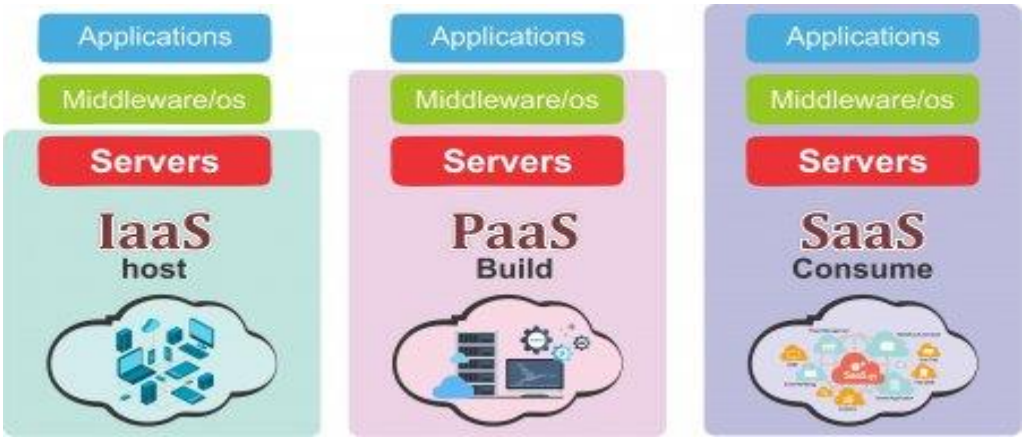


Fig: IaaS vs. PaaS vs. SaaS

4.0 CLOUD DEPLOYMENT MODELS

Cloud Deployment model gives us the information about the type of access to the cloud, i.e., where the infrastructure to deployment resides and who has the control to deploy.
It is basically taken into consideration based on several business requirements such as money, manpower etc according to the organizational necessity.

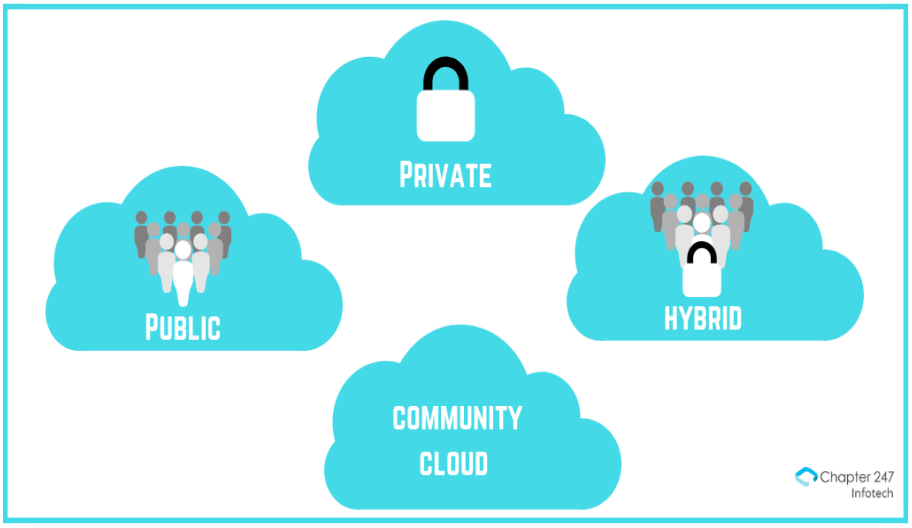


Fig: Deployment models in cloud.

Cloud deployment models are mainly of four types which are as follows:

1. Private cloud
2. Public cloud
3. Community cloud
4. Hybrid cloud

4.1 Private cloud:

ISSN: 2233-7857 IJFGCN

It is also known as ***corporate cloud*** or ***internal cloud.*** It is utilized by organizations for building and managing the data centers by external parties (off-premises) or internally (on-premises) [6].The private cloud has higher command over its infrastructure and resources for controlling the reliability, security and performance [10].Therefore, it ensures more privacy to its consumers. To ensure the management simplicity of the cloud model, it allows its consumers to arrange and handle their own workstation.
E.g.: Eucalyptus, Ubuntu enterprise cloud, Amazon virtual private cloud, Microsoft ECI datacenter and VMware cloud infrastructure models employ private cloud deployment.

4.2. Public cloud:
This is the most ubiquitous model that allows services and the system to be easily utilized by common users on subscription basis. It mainly increases the efficiency by enabling higher storage capacity by providing its users with the *multi-tenancy* solution, i.e., multiple consumers can make use of the services and infrastructure simultaneously from the shared resource pool making it inexpensive to the consumers. Therefore, it is easily scalable, elastic, location-independent and more reliable in case of infrastructure failures. Since the data as well as the resources are readily available off-site, there is minimum control over the data, network configurations and security which in turn weigh down their efficiency and reach in business scenarios [8].
E.g.: Amazon elastic compute cloud (EC2), Google AppEngine, Microsoft, IBM smart cloud enterprise and windows Azure service platform operate their hardware from the datacenters.

4.3 Community cloud:
Community cloud model allows sharing of system and resources by a cluster of several organizations in between the organization and a specific community which have common compliances, requirement and needs. The infrastructure and its services can be possessed, managed and operated by 1 or more organizations in the community, by a third-party or with a combination of them existing on or off-premises [6]. Community cloud can be implemented onsite at the customer's premises or can be outsourced to a hosting company.
E.g.: Microsoft Government community cloud, Google apps for Government, healthcare system and in scientific research scenarios.

4.4 Hybrid cloud:
Hybrid cloud is the amalgamation of two or more clouds-public, private or community clouds by allowing data and resources to be shared among them. Although the entities remain unique, they are bound together by a proprietary technology maintaining the standards [6]. It facilitates the companies to mix and match the facets of the 3 types to best suit their business requirements by balancing both the shortfalls and the benefits. Organizations opt for hybrid cloud deployment for faster delivery of new products and services. It is an excellent means to eradicate risk as it provides scalability and the cost-effectiveness of the public resources and a higher degree of private resources security. It is highly flexible as companies can choose to transfer tasks between their private and public clouds. Hybrid clouds offer better application and data portability for great outcomes

ISSN: 2233-7857 IJFGCN

E.g.: Windows Azure and VirtualMachineWare cloud.

	Public	Private	Community	Hybrid
Ease of setup and use	Easy	Requires IT proficiency	Requires IT proficiency	Requires IT proficiency
Data security and privacy	Low	High	Comparatively high	High
Data control	Little to none	High	Comparatively high	Comparatively high
Reliability	Low	High	Comparatively high	High
Scalability and flexibility	High	High	Fixed capacity	High
Cost-effectiveness	The cheapest	Cost-intensive; the most expensive model	Cost is shared among community members	Cheaper than a private model but more costly than a public one
Demand for in-house hardware	No	Depends	Depends	Depends

Tab: Comparison of different cloud deployment models.

5.0 CHALLENEGES:

Through this paper we would like to point out the challenges the organizations face when trying to adapt the cloud model. These challenges have become a major concern which questions the efficiency and the practicality in implementing the cloud mechanism.

A) *Security* :

The strongest concern that resists the users from adopting the cloud is the lack of data-security. Majority of the cloud service providers replicate the user's data which increases the data redundancy and system failure independence over a network geographically. Consumer might feel that his investment might be at risk if the cloud provider fails in providing a commitment to access the data when a service agreement is sealed and cannot meet the requisite compliance norms (policies, standards, contracts, regulation changes, etc.) [11]. Some of the major security threats include backup and storage, data leakage, unencrypted data, shared multi-tenant resources in an environment, cloning, mobility of data, data hijacking, etc.

B) *Privacy*:

Privacy is another biggest concern that is existing from a long period of time. Data privacy deals with ensuring the safety of the personal identifiable information of the users which is easily available in the cloud computing services as a result of privacy issues which pose as a serious threat to the consumer sensitive data. Privacy issues varies according to different cloud scenarios such as user service abuse, averting attacks, identity management, data audit and monitoring breach, etc.

C) *Service level Agreements* [SLA]:

Organizations those are planning to migrate to the cloud based model often face SLA issues. SLA is an agreement between the cloud service provider and the consumer which

ISSN: 2233-7857 IJFGCN

is a key factor in provisioning cloud services. SLAs are often written in favor to the providers and not the users [12] as they don't ensure the accountability for the data integrity.

D) *Migration of data*:
In order to migrate the data from the source platform to the cloud platform or trade within the existing clouds, there needs to be a certain level of expertise as the cloud architectures of the applications differ according to the various cloud service contributors.

E) *Lack of Cyber Laws*:
Utilizing cloud model has a lot of legal issues. Based on the literature survey, one of the prominent issues was the data placement [13]. How and where the Data Storage, Data processing and the Usage of the cloud takes place are the major concerned threats as the rules and laws vary widely in different parts of the world across different jurisdictions [15] ,[16], [17]. Other legal issues include data counterfeiting and traceability. When the information surpasses the internal boundaries, protection of the data cannot be guaranteed.

F) *Data Breach*:
As the data is widely accessible there is an increase in the applications and the consumers of the cloud information. Consumer demand imposes an increase in the number of access points through which even unauthorized members can retain the encrypted information available resulting in the loss of the confidentiality.

G) *Storage*:
Storage refers to the physical presence of the user's information in the cloud which can be obtainable through the entire world over any geographical location. Nowadays, majority of the organizations prefer to store their data within their premises and not far away from their place [14]. Storing of data anywhere doesn't retain the confidentiality and the liability of the data.

H) *Performance*:
The factors such as transfer rates, limited capability, Infrastructure, Internet transfer rates, service usability, etc. keep scaling the performance of the cloud model high and low irrespective of the innumerable computing services provided at any time.

I) *Dependency of Internet*:
One of the most obvious and prominent issue that the cloud consumers face is the network dependency. Due to the internet dependency factors such as the bandwidth, speed, etc. there may be interruptions and service terminations. Therefore, if there is no internet connection the user cannot make use of the cloud services.

J) *Insider access*:
The primary demerit of the cloud is that the cloud's server is readily available to the employees on whom the consumers have no control as the employee's data is not revealed to the consumers. They can alter the personal information and can misuse the confidential data effecting the consumer's reputation and economic productivity. So, the service users must ensure that their data is placed in safe hands.

K) *Service availability*:

ISSN: 2233-7857 IJFGCN

Although the clouds are designed for high availability and reliability, it is impractical to achieve 100% reliability. Some factors like natural calamities, infrastructure failures, higher traffic, lack of standards, portability across various platforms, etc. result in the service outages [18] causing inconvenience to the cloud consumers.

L) *Ease of Scalability:*

Computing services must provide the companies with the flexibility of adding or deleting the infrastructure resources when and where as needed, which is called as scalability. Clouds must be able to scale in and out rapidly as per the requirements so that no additional cost of penalties is imposed.

There are several other challenges such as power management issues, liability, trust, of governance, immaturity of standards, etc. at the service provider level, network level and the end-user levels.

CONCLUSION:

Cloud computing is a technologically influential and revolutionary computing standard in providing services over the internet facilitating cost-effectiveness, greater reliability and flexibility, on demand services to users for various organizations. Cloud computing is still is in its budding stage where the demerits and threats still exist. In this paper, we put forth the fundamental concepts and the challenges faced by both cloud service providers and the end users. Hopefully, there needs to be a proper research in establishing the set of guidelines and standards in improving the efficiency and avoiding the shortcomings.

REFERENCES:

[1] National Institute of Standards and Technology - Computer Security Resource Center – www.csrc.nist.gov

[2] http://en.wikipedia.orglwikilCloud_computing

[3] Zhang, Qi, Lu Cheng, and Raouf Boutaba, "Cloud Computing: State-of-the-Art and Research Challenges," Journal of Internet Services and Applications, vol. I, May 2010, pp.718

[4] C. Hoefer and G. Karagiannis, Taxonomy of cloud computing services, 2010.

[5] A. Lenk, M. Klems, J. Nimis, S. Tai, and T. Sandholm “What's inside the Cloud? An architectural map of the Cloud landscape”, IEEE Computer Society, pp. 23-31, 2009.

[6] P. Mell and T. Grance, The NIST definition of cloud computing. National Institute of Standards andTechnology, 53, 2009

[7] R. L. Grossman, “The case for cloud computing”, IT professional, 11, pp. 23-27, 2009.

[8] Q. Zhang, L. Cheng, and R. Boutaba, “Cloud computing: state-of-theart and research challenges”, Journal of Internet Services and Applications, 1, pp. 7-18, 2010.

ISSN: 2233-7857 IJFGCN

[9] L. Wang, J. Tao, M. Kunze, A. C. Castellanos, D. Kramer, and W. Karl, "Scientific cloud computing: Early definition and experience", IEEE, pp. 825-830, 2008

[10] https://www.flexera.com/blog/industry-trends/trend-of-cloud-computing-2020/(Cloud Computing Trends: 2020 State of the Cloud Report)

[11] European Network and Information Security Agency. ENISA. 2009. Cloud Computing: Benefits, Risks and Recommendations for Information Security URL: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment [accessed 2011-09-08] [WebCite Cache]

[12] Kerr J. , Teng K.," Cloud computing: legal and privacy issues", Journal of Legal Issues and Cases in Business

[13] K. Rafique, A. W. Tareen, M. Saeed, J. Z. Wu and S. S. Qureshi, "Cloud Computing Economics Opportunities and Challenges," 4th IEEE International Conference on Broadband Network and Multimedia Technology (ICBNMT), Shenzhen, 28-30 October 2011, pp. 401-406. doi:10.1109/ICBNMT.2011.6155965

[14] Takabi, H. 2010: "Security and Privacy Challenges in Cloud Computing Environments", The IEEE Computer and Reliability Societies, pp 24-31.

[15] A. Khalid, "Cloud Computing: Applying Issues in Small Business," International Conference on Signal Acquisition and Processing, Bangalore, 9-10 February 2010, pp. 278-281. doi:10.1109/ICSAP.2010.78

[16] J. F. Yang and Z. B. Chen, "Cloud Computing Research and Security Issues," International Conference on Computational Intelligence and Software Engineering (CiSE), Wuhan, 10-12 December 2010, pp. 1-3.

[17] Z. Mahmood, "Data Location and Security Issues in Cloud Computing," International Conference on Emerging Intelligent Data and Web Technologies (EIDWT), Tirana, 7-9 September 2011, pp. 49-54. doi:10.1109/EIDWT.2011.16

[18] Mcconnell International,"Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information"

ISSN: 2233-7857 IJFGCN