International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 01
January 2018

Cloud Computing Concept, Technology and Architecture

Ms. Sakshi
Assistant Professor Department of Computer Science and Applications, Guru Nanak College, Ferozepur Cantt, Punjab, India.

Abstract
Cloud computing has materialized as a new platform in the field of Computer Science. It is Internet-based computing, where in hardware and software resources are provided to user's on-demand. Cloud computing provides a platform with an enhanced and efficient way to store data in the cloud server with different range of capabilities and applications. Different cloud computing models allow access to information and computer resources from anywhere a network connection is available. Cloud services include online file storage, social networking sites, webmail and online business applications. It provides a shared pool of configurable computing resources, including data storage space, networks, computer processing power and specialized corporate and user applications with minimal management effort or service provider interaction. This research paper presents what cloud computing is, share some information regarding the different aspects of cloud computing, the various cloud models and the overview of the cloud computing architecture. We also discuss cloud computing features and security issue, cloud computing challenges and the future of cloud computing.

Keywords: - Cloud Computing, Its characteristic, Building Block, Architecture, Security issues.

I. Introduction

Cloud computing is one of the recently emerged technology that allows users to access infrastructure, storage, software and deployment environment [1]. IT cost reductions are achieved by offloading data and computations to cloud computing. Since the concept of cloud computing was proposed in 2006, cloud computing has been considered as the technology that probably drives the next-generation Internet revolution. The first generation cloud mainly focused on aggregating large-scale IT resources into a single cloud provider and providing users with well-managed, auto-provisioned resources and services, while increasing IT resource utilization through service consolidation. It offers improved scalability, elasticity, business agility, faster startup time, reduced management costs and just-in-time availability of resources. Cloud computing provides an easy way of accessing one's personal file or data and use application without installing it on machines by just having Internet access.

Cloud computing solutions can simplify the way in which your business operates, particularly in terms of hardware needs. Through a cloud solution you are able to connect and access the same information – but now you can connect from anywhere and enjoy a more streamlined technology installation, as shown in the graphic below.

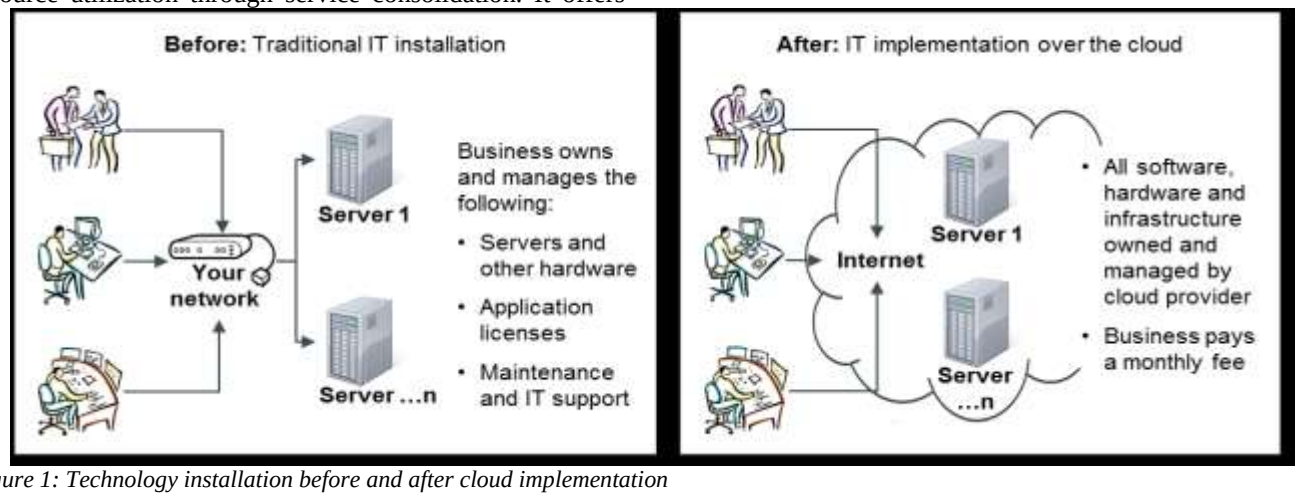


Figure 1: Technology installation before and after cloud implementation

The server and the email management software is installed on the cloud and managed by service providers. Cloud services available today vary from data storage and processing to software provision, addressing requirements for high availability and on-demand commitment-free provision of services. The resource sharing at various levels results in various cloud offerings such as infrastructure cloud (e.g., hardware, IT infrastructure management), software cloud (e.g., SaaS focusing on middleware as a service or traditional CRM as a service), application cloud (e.g., Application as a Service, UML modeling tools as a service, social network as a service) and business cloud (e.g., business process as a service). Thus, cloud computing is based on several service models such as SaaS, PaaS, DbaaS, IaaS and many more. [2].

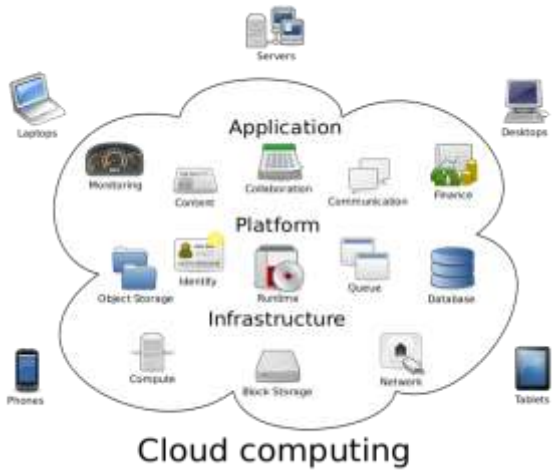


Figure 2 :Cloud Computing

This cloud computing approach eliminates the client server and grid computing. Now a days, different companies, industries, corporations and organizations prefer cloud computing instead of investing high amount of money for acquiring the servers and professional staff for maintaining this server. In cloud computing, the companies just take services from the cloud service providers as per their requirements.

It is a style of computing in which dynamically scalable and often virtualization resources are provided as a service over the internet. Cloud computing can be termed as a new paradigm for dynamic provisioning computer services supported by data centers that usually employ virtual machine (VM) technology for consolidation. With the globalization of the economy, the cross-border trade of commodities and services is continuously expanding, leading to the increasing interdependence of world economies. The economic globalization calls for globalized cloud services being provisioned in a geo-distributed manner at high availability and low cost. Therefore, a cloud vendor has to deploy data centers across all over the world. This is similar to the way used in early airline companies to expand their services by adding flight courses to a destination country to provide globalized flight courses. However, many cloud-enabled world businesses usually demand a burst of computation that exceeds the remaining computing capacity of a single cloud. Cloud Computing has widely been adopted by the industries or organizations though there are many existing issues like load balancing, virtual machine consolidation, energy management, etc. which have not been fully implemented. Central to these issues is the issue of load balancing that is required to distribute the excess dynamic local workload equally to all the nodes in the whole cloud to achieve a high user satisfaction [3]. Cloud vendors are experiencing appreciable growth rates in their business. Now-a- days, Yahoo, Gmail, Amazon Rackspace, Google, Microsoft, VMware, iCloud, Drop Box etc. are good cloud service providers. Data storage and management is one of the most fundamental services offered by cloud providers [4]. Therefore, data security has become a challenging issue of data communications recently and is the main aspect of secure data transmission over unreliable network [5, 6]. Different systems are at risk in lack of data security, which include financial systems, utilities and industrial equipment, aviation, consumer devices, large corporations, automobiles, government official work and internet. As crackers troubled away at networks and computer systems, there is a need to protect that data against unauthorized access, alternation or interchanging [7, 8]. The cloud provider must ensure that their infrastructure is secure and their clients' data and applications are protected, while the user must take measures to fortify their application and use strong passwords and authentication measures. The customers using a particular cloud, can access the resources provided by a cloud provider, according to the Service Level Agreement (SLA) given by the same cloud provider. Thus, security is considered as one of the most critical features for computer network due to sensitivity and importance of data stored.

II. ESSENTIAL CHARACTERISTICS OF CLOUD COMPUTING

Most cloud computing services are accessed through a web browser like Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox or Google Chrome. Certain cloud services could be used via a dedicated mobile app or through a browser on a Smartphone or tablet. Therefore, cloud services don't require users to have sophisticated computers that can run specialized software. In a cloud based computing infrastructure, the resources are normally in someone else's premise or network and accessed remotely by the cloud users [9, 10]. The users 'rent' it for the time they use the infrastructure [11]. Processing is done remotely implying the fact that the data and other elements from a person need to be

transmitted to the cloud infrastructure or server for processing; and the output is returned upon completion of required processing. In some cases, it might be required or at least possible for a person to store data on remote cloud servers. A cloud-based constituent relationship management (CRM) database system is an alternative to running a donor database in your office. The essential characteristics of the cloud computing is as follows:

A On-demand self service: The end user can easily access various computing capabilities, such as server time and network storage, as needed without service provider in each service.

B Broad network access: The end user's over the network can access various standard mechanisms through various thin and thick client platforms such as mobiles, laptops, desktops and workstations.

C Resource pooling: The service provider can provide various services and resources such as storage, processing, memory and network bandwidth using a multi-tenant model.

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

E Measured service: Cloud computing provide, control and optimize resource by leveraging a measure at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts). Resources can be monitored, controlled and reported transparency for both the provider and consumer of the utilized service.

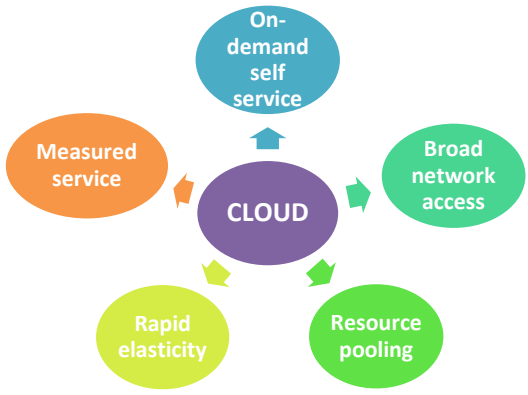


Figure 3: The Essential Characteristics of Cloud Computing

III. CLOUD COMPUTING BUILDING BLOCKS

A. DEPLOYMENT MODELS

In the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand. The Cloud Computing model has four main deployment models which are:

(i) Private Cloud:

Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization's internal enterprise datacenter. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud [12]. One of the best examples of a private cloud is Eucalyptus Systems [13].

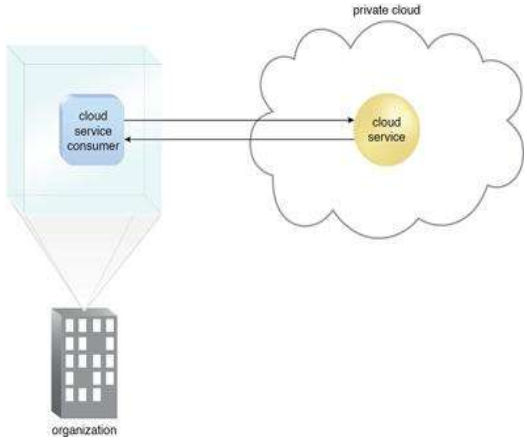


Fig4. A cloud service consumer in the organization's on-premise environment accesses a cloud service hosted on the same organization's private cloud via a virtual private network.

(ii) Public Cloud:

Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. It is typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization [14]. Public clouds are less secure than the other cloud models because it places an

additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks. Examples of a public cloud include Microsoft Azure, Google App Engine.

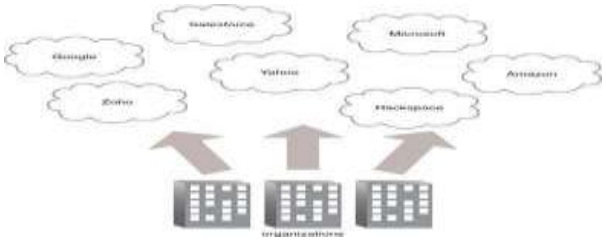


Figure 4: Show partial view of the public cloud landscape, highlighting some of the primary vendors in the marketplace.

(iii) Hybrid Cloud

Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network [15]. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Cloud provides more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems.

Hybrid cloud can describe configuration combining a local device, such as a Plug computer with cloud services. It can also describe configurations combining virtual and physical, collocated assets – for example, a mostly virtualized environment that requires physical servers, routers, or other hardware such as a network appliance acting as a firewall or spam filter. An example of a Hybrid cloud includes Amazan Web Services (AWS).

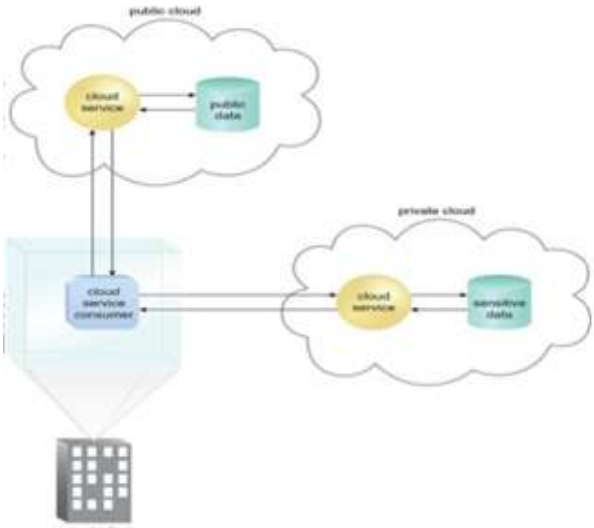
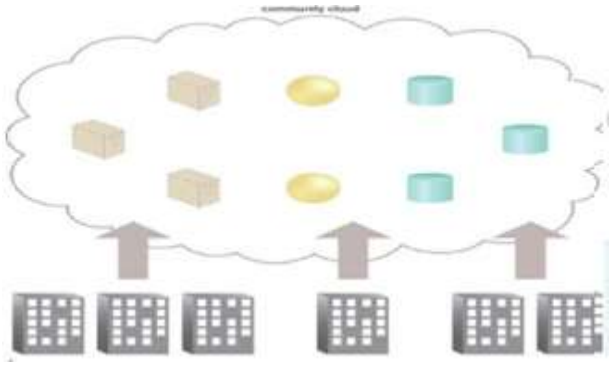


Fig5. An organization using a hybrid cloud architecture that utilizes both a private and public cloud.

(iv) Community Cloud

Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider and rarely offered cloud model. These clouds are normally based on an agreement between related business organizations such as banking or educational organizations. A cloud environment operating according to this model may exist locally or remotely. An example of a Community Cloud includes Facebook.



e 5: An example of community cloud accessing IT resources from a community cloud.

(v) JointCloud

JointCloud is a recent key project funded by China's Ministry of Science and Technology as a part of the National Key Program for Cloud Computing and Big Data, which borrows the ideas from airline alliances and aims at empowering the cooperation among multiple cloud vendors to provide cross-cloud services via software definition [16]. Prior efforts like SuperCloud and InterCloud focus on the fusion of cloud services, usually via a third-party middleware. The middleware, as an overlay, invokes different clouds and provides a uniform interface to end users. The clouds are actually unaware of the cooperation with other clouds. Different from existing multicloud models, JointCloud pays more attention to the direct collaboration among different clouds. It defines a series of rules and provides common services to enable collaboration among clouds. In JointCloud, clouds are independent while cooperating closely with one another. Just like global airline alliances Sky team and Star Alliance, there are many independent member airlines, and they work with one another closely. There are two different parts in the JointCloud architecture: the JointCloud collaboration environment (JCCE) and the peer collaboration mechanism (PCM). JCCE contains several block chain based services for enabling the cooperation among independent clouds. Based on JCCE, clouds can cooperate with one another, as long as these clouds

implement a software-defined mechanism (named PCM) and provide related APIs.

(vi) Virtual Cloud

With the development of cloud computing, more and more users prefer to run their applications on clouds such as big data processing, high-performance computing and deep learning. However, users' requirements cannot be directly satisfied by current cloud computing service model. IaaS (Infrastructure as a Service) cloud only provides users with resources such as servers, storages and networking. Users need to accomplish the environment installation with a complex configuration. In PaaS (Platform as a Service) cloud, users are provided with a cloud platform in which they can develop, manage and deliver limited applications, but they usually cannot customize the run time environment easily. Virtual cloud for special purposes is a service of Joint Cloud, which aims to provide end users with a specific cloud working environment upon several clouds just like grid computing [17], which is the collection of computer resources from multiple locations to reach a common goal. A cloud working environment has users' readily available customized software stacks, configurations and computing resources. Users can develop, test and run tasks in their working environment online through a web browser. Such a working environment is built upon a customized virtual cloud, which provides the most suitable resources from underlying clouds for the working environment. This environment could span multiple clouds seamlessly and could help applications scale out to temporarily use new resources from outside parties to deal with peak load problems. Virtual cloud is designed to provide users with cheap, flexible and easy-to-manage working environment, which is supported by virtual clusters in cloud environment, to run their own tasks. The deployment of working environment is much easier than physical clusters because of the virtual cloud's package mechanism [18]. Virtual cloud can wrap users' working environment into a small package, which can be deployed upon multiple clouds and the package can be shared with other users so that newcomers with little cluster deployment experience can directly select a proper package and deploy it to their own working environment in minutes or even seconds. Then they can work on it just like on a well-configured physical cluster. On the other hand, virtual cloud has a powerful and easy-to-use web interface; thus users can conveniently manage their working environment, process tasks and view results through a web browser. Virtual cloud could automatically build, manage, migrate and optimize a working environment based on users' requirement, by using software definition technology, making infrastructure transparent to users and scheduling resources to make a tradeoff between the quality and the cost.

(vii) Multi Cloud

Multi-Cloud denotes the usage of multiple and independent clouds by a client or a service [19]. It does not imply interconnection and sharing between clouds. The clients or their software representatives are responsible for managing resource provisioning. The selection of the best fitted place to deploy a cloud application is a complex technical issue in a Multi-Cloud that requires the introduction of a cloud resource management layer based on vendor-independent brokers and semi-automated tools (including knowledge-based selection methods for cloud services). Such a resource management system should be able to hide the complexity of service selection procedures and to control the life-cycle of the resources and services allocated to a certain application.

B. SERVICE MODELS

Cloud service deals with web-fronted applications by using various languages java, php etc. Cloud infrastructure provides user the remote infrastructures and the web fronted application are further connected to the database i.e. cloud storage [20]. The cloud computing field is commonly categorized into four main layers. These layers vary slightly from one source to the next but they can generally be summarized as infrastructure as a service, platform as a service, software as a service and data as a service.

(i) Infrastructure as a Service (IaaS)

IaaS is the foundation or bottom layer of cloud computing. It includes services like storage, backup and security. This model allows user to rent processing, storage, networks and other resources. The user can deploy a new user as a guest OS and applications. The user does not manage the complete cloud infrastructure but has the control over OS, storage, deployed applications and various network components. Some providers are Amazon EC2, GoGrid etc. IaaS users utilizes remote infrastructure, allows users to run any applications they want on cloud hardware of their own choice. While the advent of IaaS opened new territory for businesses to better manage IT hardware costs, it put developers in a challenging situation. Developers are now responsible for more of the operational work during development and test. They have to develop skills to provision, configure, manage and update hardware resources that they would have never needed in a traditional model. Amazon Web Services includes database, storage, virtual private server and support services that are available on demand by the user. Many SaaS applications rely on Amazon Web Services or other IaaS providers. Cloud-based Voice over Internet

Protocol (VoIP) telephone service is another example of IaaS. Other examples are private cloud, dedicated hosting and hybrid hosting.

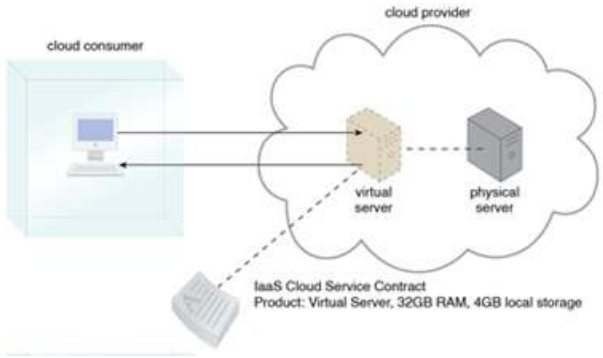


Figure 1 - A cloud consumer is using a virtual server within an IaaS environment.

(i) Platform as a Service (PaaS)

This model provides the user to deploy user built applications onto the cloud infrastructure that are built using programming languages and software tools supported by the provider. The user does not manage underlying cloud infrastructure. Platform as a Service provides platform to users to work on web application or software. It allows users to create own cloud applications using supplier-specific tools and language. The vendors of PaaS services provide a certain framework and a basic set of functions that customers can customize and use to develop their own applications. The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications using programming languages, libraries, services and tools supported by the provider. The consumer does not control the underlying cloud infrastructure including network, servers, operating systems or storage but has control over the deployed applications and possibly configuration settings for the application-hosting environment. Examples of PaaS services include Google App Engine, Force.com from Salesforce and Microsoft Azure. In a PaaS environment, the service provider not only is responsible for provisioning and managing the lower level infrastructure resources, but also for providing a fully managed application development and deployment platform. PaaS provides the developers with the appropriate flavors of operating systems, databases, middleware, software tools and managed services, usually in a multi-tenant environment. The biggest added value of PaaS is that developers are completely abstracted from the lower-level details of the environment and they can fully focus on rapid development and deployment without any worry about things like scalability, security and more that are fully managed by PaaS. In Platform as a Service, the organizations or industries have to decide at which applications are most appropriate for maintenance on the cloud. It will obviously differ from organization to organization, taking care of the critical key missions or tasks to maintain on the cloud. For instance, a company that develops software for healthcare providers is going to have different needs than a financial advisor. But even within the same industry, different organizations/sections will get different things out of the cloud.

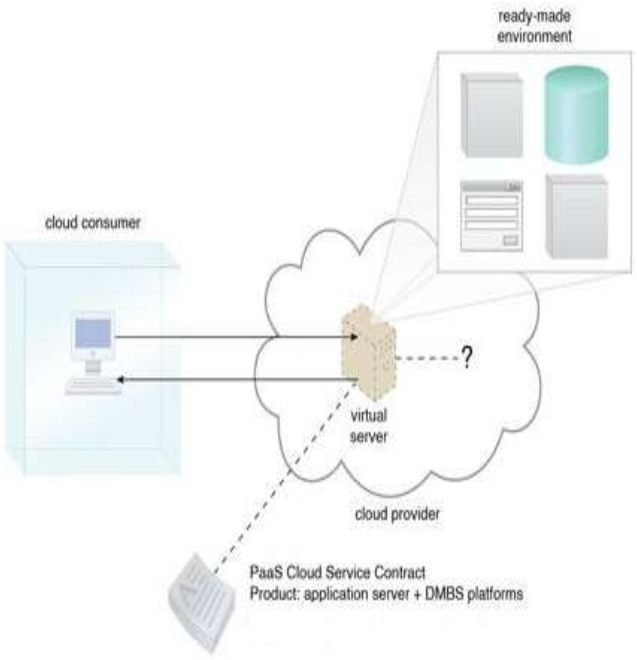


Figure 1 - A cloud consumer is using a virtual server within an PaaS environment

(iii) Software as a Service (SaaS)

It is browser initiated application software over thousands of cloud customers. In cloud, the customer need not invest in servers or software licensing. SaaS basically means any Internet-based software or service that you rent, usually on a per-user, per-month basis. It is the most common type of cloud service that small offices use. Web based application are those applications that are built using web languages like php, java,.net, etc. This model of cloud allows one to run existing online applications. The example is Google Docs. Some SaaS applications are highly customizable and we may even need a consultant to help set them up, but they generally don't require specialized knowledge for day-to-day operation and maintenance. In SaaS, an application is hosted by a service provider and then accessed via the World Wide Web by a client. Examples of SaaS include Microsoft Office 365, Google Apps, Salesforce and workstreams etc.

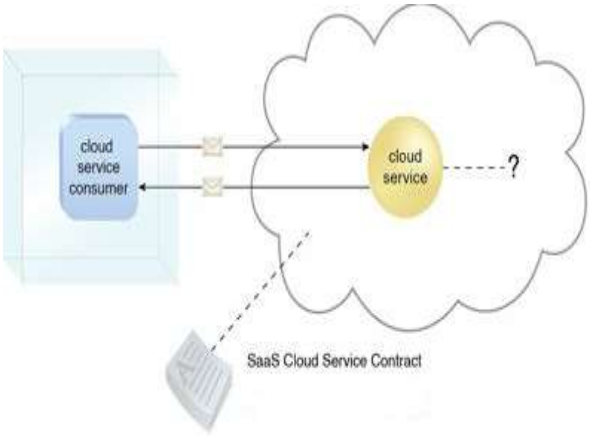


Figure 1 - A cloud consumer is using a virtual server within an SaaS environment

(iv) Data as a Service (DaaS)

The delivery of virtualized storage on demand becomes a separate Cloud service - data storage service and it could be seen as a special type IaaS. The motivation is that on-premise enterprise database systems are often tied in a prohibitive upfront cost in dedicated server, software license, post-delivery services and in-house IT maintenance. DaaS allows consumers to pay for what they are actually using rather than the site license for the entire database. In addition to traditional storage interfaces such as RDBMS (relational data base management system) and file systems, some DaaS offerings provide table-style abstractions that are designed to scale out to store and retrieve a huge amount of data within a very compressed timeframe, often too large, too expensive or too slow for most commercial RDBMS to cope with. Examples of this kind of DaaS include Amazon S3, Google BigTable and Apache HBase etc.

C. CLOUD COMPUTING ARCHITECTURE: OVERVIEW

Cloud computing can be divided into two sections, the user and the cloud. In most scenarios, the user is connected to the cloud via the internet. It is also possible for an organization to have a private cloud in which a user is connected via an intranet. However, both scenarios are identical other than the use of a private and public network or cloud [10]. The user sends requests to the cloud and the cloud provide the services

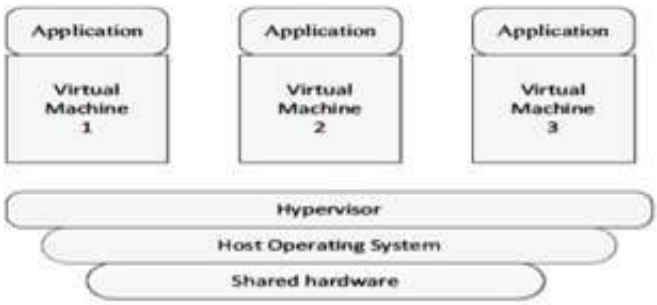


Fig. 3 Cloud Architecture [10]

Within the cloud, a central server is responsible for administering the system and in many ways functions as the operating system of the specific cloud network. Another name for this is called ―middleware‖ which is the central server for a particular cloud. Examples include Google App Engine and Amazon EC2 [21].

IV. ISSUES IN CLOUD COMPUTING

More and more information on individuals and companies is placed in the cloud. Concerns are beginning to grow about safety and security of the cloud environment [22]. Issues of cloud computing can be summarized as follows:

(i) Privacy: Cloud computing utilizes the virtual computing technology and users' personal data may be scattered in various virtual data centers rather than stay in the same physical location. Users may leak hidden information when they access cloud computing services. Attackers can analyze the critical task depending on the computing task submitted by the users.

(ii) Reliability: The cloud servers also experience downtimes and slowdowns as our local server.

(iii) Legal issues: Worries stick with safety measures and confidentiality of individual all the way through legislative levels.

(iv) Compliance: Numerous regulations pertain to the storage. Use of data requires regular reporting and audit trails. In addition to the requirements to which customers are subject, the data centers maintained by cloud providers may also be subject to compliance requirements.

(v) Freedom: Cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers.

V. SECURITY ISSUES IN CLOUD COMPUTING

Security of cloud is considered to be the most critical point and the location of the data is a major issue in the security of cloud computing. Cloud users personal data security is thus a concern in a cloud computing environment [23, 24]. The strategic policies of the cloud service provider are of highest significance as the technical security solely is not adequate to address the problem. Trust is another issue which is raised for the security concerns to use cloud service [25] because it is directly related to the authenticity and credibility of cloud computing environment. The attacks on the computer networks and the data in transit equally applies to cloud based services such as phishing, eavesdropping, sniffing and other similar attacks. DDoS (Distributed Denial of Service) attack is one common yet major attack for cloud computing infrastructure [26]. The security of the virtual machine will define the integrity and level of security of a cloud environment to greater extent. Thus, security concern involves some type of risk in the cloud computing infrastructure and it may lead to security vulnerabilities situation eventually. Any security tools or any other kind of software that are used in a cloud environment might have loopholes in security, which would pose the security risks in the infrastructure of cloud itself. Data security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among organizations, enterprises and other types of institutions, businesses, government agencies and individuals [27]. Storing of data on remote cloud servers gives the following three sensitive states that are of particular concern within the operational context of cloud computing:

(i) The transmission of personal sensitive data to the cloud server,
(ii) The transmission of data from the cloud server to clients' computers and
(iii) The storage of clients' personal data in cloud servers which are remote server not owned by the clients.

All the above three states of cloud computing are severely prone to security breach that makes the research and investigation within the security aspects of cloud computing practice. Data storage and security has become a challenging issue of cloud computing recently and therefore, security is considered as one of the most critical features for computer network due to sensitivity and importance of data stored [28]. Data security involves many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database [29]. As crackers troubled away at networks and computer systems, there is a need to protect that data against unauthorized access, alternation or interchanging [30]. The cloud provider must ensure that their infrastructure is secure and their clients' data and applications are protected, while the user must take measures to fortify their application and use strong passwords and authentication measures. The conventional methods of encryption are employed to maintain the data security [31]. Network security starts with authenticating the user, commonly with a username and a password, this is sometimes termed one-factor authentication. With two factor authentication, a security token or 'dongle', an ATM card or a mobile phone is used [32, 33]. With three-factor authentication, a fingerprint or retinal scan is used. Once authenticated, firewall forces access policies such as what services are allowed to be accessed by the network users. An anomaly based intrusion detection system may also monitor the network and traffic for suspicious content or behavior and other anomalies to protect resources, e.g. from denial of service attacks or an employee accessing files at strange times. Due to the multi-tenancy arrangement of cloud services, the security challenge is much more difficult. Although, there are many security and privacy frameworks being developed and implemented, none offers a complete security and privacy solution. The initial reaction of the community to the security issues of cloud computing was that these could be resolved using existing techniques inherited from conventional IT systems or even distributed systems that are the ancestors of cloud computing environments [34]. Given the number of systems now dependent on cloud implementations, including the rapidly evolving Internet of Things (IoT) and Big Data, this is rather concerning. Legislative and regulatory bodies have taken notice of the adverse impact of security and privacy breaches on companies, individuals and society as a whole, and these agencies are proposing to levy higher punitive fines on companies who suffer such breaches. Accountability from all the users involved in cloud ecosystems is often aided by service level agreements. The cloud service provider should take a robust attitude to vetting all staff, but this level of rigor may not apply to sub-contractors. The threat environment is often not well understood by companies, sometimes resulting in a far less robust approach to the risks involved. Even though cloud computing has found versatile ground as an economic model and is attracting a lot of investment; many are still reluctant to use cloud services because of several security, privacy and trust issues that have emerged. Hence, a need to re-consider security, privacy and trust concerns in the context of the cloud computing paradigm arises.

VI. CONCLUSION

Cloud Computing, envisioned as the next generation architecture of IT Enterprise is a talk of the town these days. The way cloud has been dominating the IT market, a major shift towards the cloud can be expected in the coming years. Cloud computing offers real benefits to companies seeking a competitive edge in today's economy. Many more providers are moving into this area, and the competition is driving prices even lower. Attractive pricing, the ability to free up staff for other duties, and the ability to pay for ―as needed services will continue to drive more businesses to consider cloud computing. Mobile cloud computing is expected to emerge as one of the biggest market for cloud service providers and cloud developers.

Although Cloud computing can be seen as a new phenomenon which is set to revolutionize the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception. Cloud service providers need to inform their customers on the level of security that they provide on their cloud. This research effort presents an overview of Cloud Computing, building blocks of Cloud Computing which includes different models of cloud computing, overview of Cloud Computing architecture and Cloud Computing entities. Furthermore, security issues which are currently faced in the Cloud computing were also highlighted.

Cloud computing has the potential to become a front runner in promoting a secure, virtual and economically viable IT solution in the future. As the development of cloud computing technology is still at an early stage, this research effort will provide a better understanding of the design challenges of cloud computing, and pave the way for further research in this area.

REFERENCES

[1] Kumar, V., "Brief review on cloud computing", International Journal of Computer Science and Mobile Computing, Vol. 5, issue 9, pp. 01-05, 2016.

[2] Adamuthe, A.C., Salunkhe, V.D., Patil, S.H. and Thampi, G.T., "Cloud computing – A market perspective and research directions", International Journal of Information Technology and Computer Science, Vol. 10, pp. 42-53, 2015. DOI: 10.5815/ijitcs.2015.10.06.

[3] Yamini, R., "Power management in cloud computing using green algorithm", IEEE-International conference on Advances in Engineering, Science and Management, March 30-31, 2012, pp. 128-133, 2012.

[4] Verma, C.P., Chaudhary, N. and Rastoagi, N., "Analyzing cloud storage database management", International Journal of Innovative Computer Science and Engineering, ISSN: 2393-8528, Vol. 1, issue 1, pp. 06-09, 2014.

[5] Sindhu, S. and Sindhu, D., "Cryptographic algorithms: Applications in network security", International Journal of New Innovations in Engineering and Technology, ISSN: 2319-6319, Vol. 7, issue 1, pp. 18-28, 2017.

[6] Sharma, M., Husain, S. and Ali, S., "Cloud computing risks and recommendations for security", International Journal of Latest Research in Science and Technology, ISSN: 2278-5299, Vol. 6, pp. 52-56, 2017.

[7] Krombholz, K., Hobel, H., Huber, M. and Weippl, E., "Advanced social engineering attacks", Journal of Information Security and Applications, Vol. 22, pp. 113-122, 2015.

[8] Zeng, W., Koutny, M., Watson, P. and Germanos, V., "Formal verification of secure information flow in cloud computing", Journal of Information Security and Applications, Vol. 27-28, pp.103-116, 2016.

[9] Petre, R., " Data mining in cloud computing", Database Systems Journal, Vol. 3, issue 3, pp. 67–71, 2012.

[10] Singh, S. and Jangwal, T., "Cost breakdown of public cloud computing and private cloud computing and security issues", International Journal of Computer Science and Information Technology, Vol. 4, issue 2, pp. 17-31, 2012.

[11] Rashmi, Sahoo, G. and Mehfuz, S., "Securing software as a service model of cloud computing: Issues and solutions", International Journal on Cloud Computing: Services and Architecture, Vol. 3, issue 4, pp. 01-11. Doi: 10.5121/ijccsa.2013.3401, 2013.

[12] S. Arnold (2009, Jul.). ―Cloud computing and the issue of privacy.‖ KM World, pp14-22. Available: www.kmworld.com [Aug. 19, 2009].

[13] B. R. Kandukuri, R. Paturi V, A. Rakshit, ―Cloud Security Issues‖, In Proceedings of IEEE Internati onal Conference on Services Computing, pp. 517-520,

[14] A Platform Computing Whitepaper. ―Enterprise Cloud Computing: Transforming IT.‖ Platform Computing, pp6, 2010.

[15] Global Netoptex Incorporated. ―Demystifying the cloud.Important opportunities, crucial choices.‖ pp4-14. Available: http://www.gni.com [Dec. 13, 2009].

[16] Cao, D-G., An, B., Shi, P-C. and Wang, H-M., "Providing virtual cloud for special purposes on demand in JointCloud computing environment", Journal of Computer Science and Technology, Vol. 32, issue 2, pp. 211-218, 2017.

[17] Foster, I., Zhao, Y., Raicu, I. and Lu, S., "Cloud computing and grid computing 360-degree compared", In Proceedings Grid Computing Environments Workshop, Nov. 2008.

[18] Sun, D.W., Chang, G.R., Gao, S., Jin, L.Z. and Wang, X.W.. "Modeling a dynamic data replication strategy to increase system availability in cloud computing environments", Journal of Computer Science and Technology, Vol. 27, issue 2, pp. 256-272, 2012.

[19] Munteanu, V. I., Şandru, C. and Petcu, D., "Multi-cloud resource management: cloud service interfacing", Journal of Cloud Computing Advances, Systems and Applications, Vol. 3, pp. 3-8, 2014. DOI: 10.1186/2192-113X-3-3.Wei, Y. and Blake, M.B., "Service-oriented computing and cloud computing: Challenges and opportunities". IEEE Internet Computing, Vol. 14, issue 6, pp. 72-75. 2010.

[20] Wei, Y. and Blake, M.B., "Service-oriented computing and cloud computing: Challenges and opportunities". IEEE Internet Computing, Vol. 14, issue 6, pp. 72-75. 2010.

[21] Ertaul, L. and Singhal, S. 2009. Security Challenges in Cloud Computing. California State University, East Bay. Academic paper http://www.mcs.csueastbay.edu/~lertaul/Cloud%20Security%20CamREADY.pdf

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

[23] Joint, A., Baker, E. and Eccles, E., "Hey, you, get off of that cloud?" Computer law and security Review, Vol. 25, pp. 270-274, 2009.

[24] King, H.J. and Raja, "protecting the privacy and security of sensitive customer data in the cloud", Computer Law and security reviews, Vol. 28, pp. 308-319, 2012.

[25] Abbadi, I.M. and Martin, A., "Trust in the Cloud",Information Security Technical Report, Vol. 16, pp. 108-114, 2011.

[26] Dou, W, Chen, Q. and Chen J., "A confidence-based filtering methods for DDoS attack defense in Cloud environment", Future Generation Computer System, Vol. 29, pp. 1838-1850, 2013.

[27] Shahzad, F., "State-of-the-art survey on cloud computing security challenges, approaches and solutions", Procedia Computer Science, Vol. 37, pp. 357-362, 2014.

[28] Ryan, M.D., "Cloud computing security: The scientific challenge and a survey of solutions". The Journal of Systems and Software, Vol. 86, pp. 2263-2268, 2013.

[29] Sindhu, S. and Sindhu, D., "Cryptographic algorithms: Applications in network security", International Journal of New Innovations in Engineering and Technology, ISSN: 2319-6319, Vol. 7, issue 1, pp. 18-28, 2017.

[30] Bollavarapu, S. and Gupta, B., "Data security in cloud computing", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, issue 3, pp. 1208-1215, 2014.

[31] Khan, S.S. and Tuteja, R.R., "Security in cloud computing using cryptographic algorithms", International Journal of Innovative Research in Compute and Communication Engineering, Vol. 3, issue 1, pp. 148-154, 2015.

[32] Mason, S. and George, E., "Digital evidence and cloud computing", Computer Law and Security Review, Vol. 27: pp. 524-528, 2011. doi:10.1016/j.clsr.2011.07.005.

[33] Yassin, A.A., Jin, H., Ibrahim, A., Qiang, W. and Zou, D., "Efficient pass word based two factors authentification in cloud computing", International Journal of Security and its Applications, Vol. 6, issue 2, pp. 143-148, 2012.

[34] Chaudhary, N., "An overview of issues and data security expert reveal for cloud computing", International Journal of Computer Science and Mobile Computing, Vol. 6, issue 3, pp. 154-159. 2017.