Glimpse of Cloud Computing

Anushka Gaur
CEC, Landran, Punjab
meanushkagaur@gmail.com

Anurag Jain
CEC, Landran, Punjab
er.anuragjain14@gmail.com

Abstract: *In this paper, the concept of cloud computing has been studied. The service provider must ensure that the infrastructure and applications are protected and must take actions to reinforce user's application and use strong passwords and authentication measures. In the first part, a brief introduction to the cloud computing has been given. It includes a definition of cloud computing given by NIST and other scholars. In the next section, the architecture and various service models, as well as deployment models provided by cloud computing, has been discussed. This is followed by the working of the cloud which includes the concept of virtualization. Then the light has been put on its major application areas. In the next part, its advantages and disadvantages have been highlighted.*

Keywords: Cloud Computing, NIST, Authentication, Virtualization.

I. INTRODUCTION

A few years back, people used to run applications and programs by downloading the software's on a physical device like a computer and the user himself was responsible for all the necessary updates such as security updates. Users could send files as email attachments and whatever the work was required to be done that had to be done by one user at a time and that generally used to create a mess of conflicting file content and other data. Moreover, even the large database was not sufficient to meet the demand of storing an increasing amount of data. So, companies decided to move all the data to the cloud where all the files are stored centrally. Cloud computing is a new trend and companies have started using the concept of cloud computing.

Cloud is basically a common virtual database [1] which not only store files or other data but also contain a shared pool of resources. Here the resource can be a software, any service or any other kind of application or some data. Moving to the cloud gives access to everyone. So, with this new trend, the users are now no longer responsible for installing software or any kind of application on to their physical devices instead of that software or that application can be directly accessed whenever required. Hence, it has been given the name" On-demand Computing" [1].

The beauty of cloud computing lies within the fact that a consumer need not buy a software or an application because the consumer can use it by directly logging on to a particular website and need to pay only for that particular time for which the resources have been being used by the consumer. Service providers take care of regular software updates so the consumer need not worry about wasting time in maintaining the software. This makes the consumer free and allows him to focus on the things that matter.

Hence, cloud computing is purely a business activity because the consumer simply pays for the requested subscription [2].So cloud computing cuts out the high costs of hardware. The only thing that is required by a consumer on a physical device is the internet connectivity. Once there is an internet connection then the consumer can do work from anywhere. The most popular social networking sites like Facebook are also an example of cloud computing implementation because when a user is updating a status, cloud technology is being used at that time. Checking bank balance on a phone? The user is in the cloud again.

Definition

Different scholars have given different definitions of cloud computing. The definition given by Vangie Beal is" Cloud computing is a type of computing that relies on sharing computing resources in place of having local servers or personal devices to handle applications"[1].Cisco defines cloud computing as" IT resources and services that are abstracted from the underlying infrastructure and distributed when required and at scale in a multitenant environment"[3].In Cloud Computing, the word cloud is used to describe the "internet"[3]. So, the term cloud computing can be defined as that kind of computing that is based on the internet, where several services such as servers, storage, and applications are delivered to the computers and other physical

devices of an organization through the internet[4] Amazon EC2(Elastic Computer cloud) is an example of a commercial web service that provide computing resources on lease to the customers[5].NIST(National Institute of Standards And Technology) issued a different definition in September,2011.NIST defined Cloud Computing as "a model for enabling ubiquitous, convenient , on demand network access to a shared pool of compatible computing resources(example network , servers, storage, applications, and services)that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of three service models and four deployment models [6]. Hence, by concluding cloud computing can be defined as the use of computing resources which are placed in a data center and are accessed via the internet from any location.

Architecture
The architecture of cloud computing includes all those components, subcomponents and elements that are used for computing [7].The architecture of cloud computing includes three types of service models. These are named as SaaS, PaaS, and IaaS. The below figure represent these models:
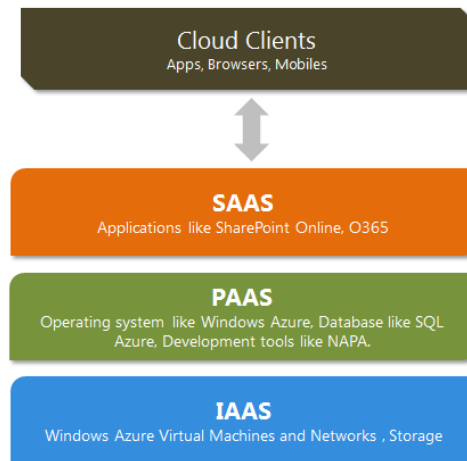

Fig1 [9]: Cloud Computing Service Model

Software as a Service (SaaS): This service model allows a consumer to use a commercial software [8] or a pre-developed software on pay per use basis. It means more usage more cost and less usage less cost. So, there is no need to download the software on the physical machine. Hence this service model allows multiple consumers to use the same software at the same time[8].The consumer is free from doing all kind of settings or configurations[8].The cloud provider will do all the settings and the desired configuration on the behalf of the consumer. Example-Gmail.

Platform as a service (PaaS): This service model allows the consumer to develop their own program or application by using any programming language or tools provide by the cloud provider. In this, the consumer has control over the application and the configuration settings of the application that is being developed by the consumer.

Infrastructure as a service (IaaS): In this service, model administrators provide infrastructure to the consumers or developers so as to support their development operations. It means one can outsource the elements of infrastructure like storage, servers, networks etc. to a cloud provider like Microsoft [9]. Here Microsoft acts as an administrator. For example, using Microsoft Windows Azure one can set up new windows server and Linux virtual machines and can adjust the usage as per the requirement [9].
Apart from these service models the architecture of cloud computing also includes the deployment models which further include four types of cloud namely public cloud, private cloud, community cloud and hybrid cloud.

Public cloud: It is that type of cloud in which all the computing resources are made available to everyone over a public network by the cloud service provider. Since it is made available to all the groups of the general public at a very low cost so it is less secure as compared to private cloud.

Private cloud: In the case of private cloud all the computing resources are made available to a particular organization. It means that only the employees of that organization can have access to those computing resources. All other public is not allowed to gain access to those computing resources which are owned by that organization. Hence this type of cloud offers greater security but at a high cost.
Community cloud: It is that type of cloud in which the computing resources are made available to a group of people with the same objective, the can either be concerned with the security, privacy or performance related issues. It is different to the private cloud in the sense that it includes multiple organizations participating while in the case of private cloud there is only a single organization that owns a particular cloud.

Hybrid cloud: A hybrid cloud is made by the combination of two or more other types of clouds. For example, the more critical data can be moved to the private cloud while the less critical data can be placed in the public cloud.

How does a cloud work?
After getting a basic idea of the architecture of cloud computing the next thing that comes into the picture is that how does it work? As we have an internet provider, in the same way, we also have cloud provider companies such as Google, Microsoft etc. These cloud provider companies make all the resources (such as a software, hardware, servers, storage space etc.) available to individuals or any organization at the same time. It means that all the persons or business groups are sharing those resources at the same time. Companies have moved their data to the cloud so that different employees can access the same resource at the same time. The cloud is basically a data center including a large number of servers and other computing resources that reside on the internet [10].So, internet connection is the only thing that is required to access the computing resources residing on the cloud. Because multiple organizations can access the same resource at the same time so the cost of buying software is reduced. Another thing that is associated with the cloud is that there is no restriction on the number of users using the cloud services.

Virtualization in cloud computing
Virtualization is the key concept behind cloud computing. Virtualization creates an illusion of the resources. It means that virtualization is the use of hardware and software to create the perception that one or more entities exist although they are not physically present in reality [11]. Virtualization increases the hardware utilization as it becomes very easy to share resources among multiple users without letting the users know that the resources they are using are just an illusion of the physical resources[12].The figure below represents the process of virtualization in cloud computing.
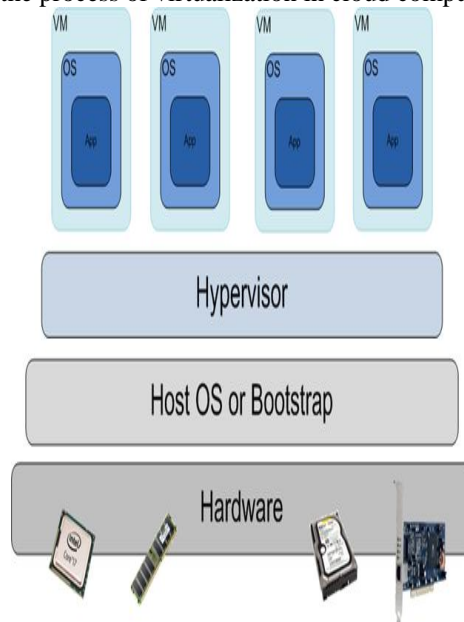

Fig2 [11]: Virtualization Process in Cloud Computing

Cloud computing makes use of virtual machine monitor (VMM) or virtual manager or hypervisor, which is the technology behind cloud computing and which separates computer environment from the actual physical environment [13]. The hypervisor is responsible running multiple virtual machines and the machine on which virtual machines run is called host machine and the virtual machine itself is called as guest machine [11].

Application Areas
Some of the major areas in which the cloud computing is used are:

Commercial Purpose: The cloud computing is purely a business activity because the companies need not buy expensive software or hardware as all of them is available on lease.

Entertainment: The cloud offers a large storage space so that a user can store all his media pictures and videos on the cloud and can request them when required.

Education and information: Microsoft and other vendors are starting to position their cloud offerings to schools. Microsoft points to help create online classrooms [14].

Communication: The Gmail and the Facebook which are almost the best way to communicate are using the cloud computing technology.

Medical: The cost of health-care services can be reduced by ensuring efficient use of resources and standardizing health-care processes. Mobile cloud computing is a promising technology that can provide good solutions to those issues. The use of mobile devices support convenient access
To patient-related information and effective communications between medical team members [15].

Advantages
The cloud computing offers various benefits in various forms which have made all the business organizations and IT companies to move all their data to the cloud. The advantages offered by cloud computing are as follows:

Pay-per-use: Because the cloud computing is based on a pay-per-use basis so this makes it cost efficient up to some extent as it cuts the need to buy a software.

Shared Resources: The cloud has a shared pool of different computing resources which allow different consumers to access even the same resource at the same time. It means that the resources are being shared by different organizations simultaneously.

Availability: The different computing resources are available everywhere to everyone at any point in time [9].
No Maintenance: The consumer is free from doing any kind of updates or maintenance as this is the responsibility of the cloud provider [16].

On Demand Service: The main benefit of cloud computing is that the resources are made available to the consumers as soon as they demand them and are released after the successful fulfillment of their demand[6].

Broad Network Access: The cloud computing provides a broad network access to the resources. It means that the resources can be accessed from almost everywhere in the world [6].

Easy Access: The method used to access the resources of the cloud is very easy [6].

Measured Service: The cloud provider will keep track of the services offered to the users. It means that the time period for which a user is allowed gain access to the resources is always being measured by the cloud provider and the resources have to be released after that[6].

Unlimited Storage: The capacity of the cloud to store information is almost unlimited. In fact, the cloud came into existence to cope up with the storage problems that were being faced by the organizations [6].

Backup and Recovery: If the data gets lost from the physical device then there is no need to worry about the lost data if the same was kept on the cloud also because cloud always keeps a backup of the data hence making its recovery easy in case of data lost[6].

Disadvantages
The use of cloud computing is increasing rapidly because of its several advantages. But apart from the above-discussed advantages, there are some problems too. The main problems that are being faced by organizations using cloud computing are:

Security: As the companies have to send all their sensitive information to the cloud service provider so their sensitive data is always at a risk [16].

Privacy: The privacy of the companies can be compromised as all the information is sent to the cloud service provider.

Power consumption: The other issue related to the cloud computing is that it consumes the great power of the physical devices such as a smartphone.

Technical Issues: Sometimes there can be some technical issues like servers might be down so at that time it becomes difficult to gain access to the resources at any time and from anywhere e.g. non-availability of services can be due to denial of service attack [17].

Strong Internet Connection: To use the technique of cloud computing there should always be a strong internet connection without which we would not be to take advantage of the cloud computing.

Security Issues

To keep data associated with the cloud free from threat and danger is a major point of concern. Cloud computing security encompasses protection of data, applications, and other important stuff. Some of the main security threats that are frequent to arise are:

Information security: The data provided to the cloud provider is always at risk. Information security is related to data integrity, data confidentiality and data access controllability.

- **Data Integrity:** Data integrity is reflected by the absence of any kind of modification. For instance when a client updates a record in the database then it should not be changed by an intruder. It means that data integrity ensures that the data remains unchanged.

- **Data confidentiality:** Confidentiality is said to achieve when only authorized users are allowed to access the sensitive data. It means that the data is protected against the unauthorized attempt over the sensitive data. However, to achieve confidentiality in cloud computing is a tough task.

- **Data access control:** It signifies that different persons have different access permissions over the data. In other words, it is a way of restricting the access to the sensitive data.

Network security: Network security is a way to protect and control the access to the files inside the network and also to protect the network itself from different attacks such as:

- **DoS and DDoS**: A distributed denial of service attack (DDoS) is said to occur when various attackers flood the bandwidth or resources of a targeted system with unwanted traffic by means of different and new methods. In this type of attack, the attacker first tries to gain access to a user account on multiple hosts across the Internet and then installs and runs a slave program at each compromised system that silently waits for commands from a master program. The master program then interacts with the slave programs, providing instructions to each one of them to launch a denial-of-service attack. The resulting attack is generally ruination since it comes from various attacking hosts at the same interval of time.

- **Spoofing (Identity spoofing or IP Address spoofing):** When an internet connected device sends IP datagrams into the network then such internet data packets contains the sender's IP address. In such a case if the attacker succeeds in gaining control over the software running on a network device, then undoubtedly they will modify the device's protocols to some other IP address. This act of modifying IP is known as IP spoofing. When an IP address on a datagram becomes spoofed, it makes it difficult to locate the true sender host. The solution for spoofing is adapting filtering. Generally, routers are responsible for performing this. Routers doing filtering detect the IP address of datagrams and detect whether the source addresses that are reachable or not via that interface. If the source address does not come under the valid range, then such packets will be discarded otherwise they will be allowed.

- **Sniffing:** Sniffing of data packets is the interpolating of data packets within a network. A sniffer program performs at the Ethernet layer in aggregation with network interface cards (NIC) to imprison all the incoming and outgoing traffic from the internet host site. Also, if any of the Ethernet NIC cards are in promiscuous mode, the sniffer program will pick up all communication packets floating by anywhere near the internet host site. A sniffer placed on any backbone device, inter-network link or network aggregation point will, therefore, be able to monitor a whole lot of traffic. Most of the packet sniffers are passive and they listen all data link layer frames passing by the device's network interface. There are dozens of freely available packet sniffer programs on the internet. The more sophisticated ones allow more active intrusion.

The key to detecting packet sniffing is to detect network interfaces that are running in promiscuous mode. Sniffing can be detected two ways:

1. Host-based: Software commands exist that can be run on individual host machines to tell if the NIC is running in promiscuous mode.
2. Network-based: Solutions tend to check for the presence of running processes and log files, which sniffer programs consume a lot of. However, sophisticated intruders almost always hide their tracks by disguising the process and cleaning up the log files.

The best countermeasure against sniffing is end-to-end or user-to-user encryption.

Hijacking (man-in-the-middle attack: This is a technique that takes advantage of a weakness in the TCP/IP protocol stack, and the way headers are constructed. Hijacking occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data. Man-in-middle attacks are like someone assuming your identity in order to read your message. The person on the other end might believe it is you because the attacker might be actively replying as you, to keep the exchange going and gain more information.

Proposed Solution

Although there are many problems with the cloud computing but the main issue is the security of the data stored in the cloud. There is a large amount of data present in the cloud. All the data need a different kind of security levels because different people

have different access to the data. So, to provide security to the data we may need strong and different security measures for different threats which will help in protecting data present in the cloud.

II. CONCLUSION AND SCOPE

According to this study, the cloud computing is a type of internet based computing which allow various resources to be shared among different users. Users gain access to the resources for a specific period of time on a pay per use basis and this help to reduce the cost of buying the software. A great future of cloud computing is expected as it has transformed the way people used to gain access to the computing resources. Putting all the data on the cloud has changed the trend of the business activities also. Hence it can be concluded that cloud computing has a great potential in increasing the utilization of the computing resources.

REFERENCES

[1] Nesrine Kaaniche, Aymen Boudguiga, Maryline Laurent,"ID-Based Cryptography for Secure Cloud Data Storage, "Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference

[2] Neha Tirthani, GanesanR,"Data Security in Cloud Architecture Based on Diffie-Hellman and Elliptical Curve Cryptography," International Association for Cryptologic Research, Nov 2013.

[3]Farzad Sabahi,"Cloud computing Security threats and responses "Communication Software and Networks (ICCSN).2011 IEEE 3rd International Conference.

[4] Deyan Chen, Hong Zhao," Data Security and Privacy Protection Issues in Cloud Computing,"2012 IEEE International Conference on Computer and Electronics engineering.

[5] Priyanka Ora and Dr. P.R.Pal, "Data Security and Integrity in Cloud Computing Based On RSA Partial Homomorphic and MD5 Cryptography" IEEE International Conference on Computer 2015.

[6] Shakeeba S. Khan, Prof.R.R. Tuteja, Security in Cloud Computing using Cryptographic Algorithms, Vol. 3, Issue 1, January 2015

[7] Seny Kamara and Kristin Lauter," Cryptographic Cloud Storage," June 2010.

[8] Prof Swarnalata Bollavarapu, Bharat Gupta, 'Data Security in Cloud Computing', Volume 4, Issue 3, March 2014

[9] Calheiros, Rodrigo N., et al. & quot; Cloud Sim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms & quot; Software: Practice and Experience 41.1 (2011): 23-50.

[10] Hay, B., Nance, K., & Bishop, M. (2011, January). Storm clouds rising: security challenges for IaaS cloud computing. In System Sciences (HICSS), 2011 44th Hawaii International Conference on (pp. 1-7). IEEE.

[11] Curran, K., Carlin, S., & Adams, M. (2012). Security issues in cloud computing. Cloud computing for teaching and learning: strategies for design and implementation. IGI Global, Hershey, Pennsylvania, USA, 200-208.

[12] Kaur, R., & Kinger, S. (2014). Analysis of security algorithms in cloud computing. International Journal of Application or Innovation in Engineering and Management, 3(3), 171-6.

[13] Nigoti, R., Jhuria, M., & Singh, S. (2013). A Survey of Cryptographic Algorithms for Cloud Computing.

[14] Mace, J. C., Van Moorsel, A., & Watson, P. (2011, June). The case for dynamic security solutions in public cloud workflow deployments. In 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W) (pp. 111-116). IEEE.

[15] Shah, J., & Saxena, V. (2011). Performance Study on Image Encryption Schemes. ArXiv preprint arXiv: 1112.0836. Performance efficiency and security measures of some encryption 20 algorithms. International Journal of Engineering Research and Applications (IJERA) ISSN, 2248-9622.

[16]Li, Yibin, et al. & quot; Intelligent cryptography approach for secure distributed big data storage in cloud computing. & quot; Information Sciences (2016).

[17] Kaur, R., & Kinger, S. (2014). Analysis of security algorithms in cloud computing. International Journal of Application or Innovation in Engineering and Management, 3(3), 171-6.