"A Research upon Numerous Improvements and Possibilities of Cloud Computing"

Rajkumar

Research Scholar, Bundelkhand University, Jhansi

Abstract – Cloud computing is a globalized concept and there are no borders within the cloud. Computers used to process and store user data can be located anywhere on the globe, depending on where the capacities that are required are available in the global computer networks used for cloud computing. Because of the attractive features of cloud computing many organizations are using cloud storage for storing their critical information. The data can be stored remotely in the cloud by the users and can be accessed using thin clients as and when required. One of the major issue in cloud today is data security in cloud computing. Storage of data in the cloud can be risky because of use of Internet by cloud based services which means less control over the stored data. One of the major concern in cloud is how do we grab all the benefits of the cloud while maintaining security controls over the organizations assets.

A common understanding of "cloud computing" is continuously evolving, and the terminology and concepts used to define it often need clarifying. Press coverage can be vague or may not fully capture the extent of what cloud computing entails or represents, sometimes reporting how companies are making their solutions available in the "cloud" or how "cloud computing" is the way forward, but not examining the characteristics, models, and services involved in understanding what cloud computing is and what it can become.

Cloud computing has formed the conceptual and infrastructural basis for tomorrow's computing. The global computing infrastructure is rapidly moving towards cloud based architecture. While it is important to take advantages of could base computing by means of deploying it in diversified sectors, the security aspects in a cloud based computing environment remains at the core of interest. Cloud based services and service providers are being evolved which has resulted in a new business trend based on cloud technology.

----------♦----------

INTRODUCTION

Cloud computing is a model which provides a wide range of applications under different topologies and every topology derives some new specialized protocols. In this research study, we will present an introduction to a cloud computing that is expected to be adopted by governments, manufacturers and academicians in the very near future. It directly affects the company, government and convenience to the small user. It is the technology of building a robust data security between CSP and User. This promising technology is literally called Cloud Data Security. In this research, an introduction to the technology of Cloud Computing, TPA, data security and security algorithm of different papers will be presented.

Cloud computing is a Kind of network where user can use services provided by Service provider on pay per use bases. It is a research area which provides a wide range of applications under different topologies where every topology computing that is expected to be adopted by government, manufacturers and academicians in the near future.

Cloud computing is receiving a great deal of attention, both in publications and among users, from individuals at home to the U.S. government. Yet it is not always clearly defined.1 Cloud computing is a subscription-based service where you can obtain networked storage space and computer resources. One way to think of cloud computing is to consider your experience with email. Your email client, if it is Yahoo!, Gmail, Hotmail, and so on, takes care of housing all of the hardware and software necessary to support your personal email account. When you want to access your email you open your web browser, go to the email client, and log in. The most important part of the equation is having internet access. Your email is not housed on your physical computer; you access it through

an internet connection, and you can access it anywhere. If you are on a trip, at work, or down the street getting coffee, you can check your email as long as you have access to the internet. Your email is different than software installed on your computer, such as a word processing program. When you create a document using word processing software, that document stays on the device you used to make it unless you physically move it. An email client is similar to how cloud computing works. Except instead of accessing just your email, you can choose what information you have access to within the cloud.

The economic benefits of using cloud storage and cloud computing are appealing enough to promote adoption of these technologies, hence their use is likely to increase over time . In this situation, there is a risk that the economic benefits obtained today through the rapid adoption of cloud technologies will in some cases be compensated or even overcompensated by losses resulting from unexpected lack of availability as well as theft and corruption of data.

In cloud computing data and applications are maintained with the use of central remote server and internet and allow consumers to use the applications without installating and also with the help of internet cloud computing allows customers to access their personal files which are stored in some other computer.

Yahoo email, Gmail, or Hotmail etc are examples of cloud computing. The email management software and the server are fully managed and controlled by the CSP Google, Yahoo etc and are all on the cloud.

Recent developments in the field of could computing have immensely changed the way of computing as well as the concept of computing resources. In a cloud based computing infrastructure, the resources are normally in someone else's premise or network and accessed remotely by the cloud users (Petre, 2012; Ogigau-Neamtiu, 2012; Singh & jangwal, 2012).

Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. There are four basic cloud delivery models, as outlined by NIST (Badger et al., 2011), based on who provides the cloud services.

CLOUD COMPUTING INFRASTRUCTURE

The term cloud computing is rather a concept which is a generalized meaning evolved from distributed and grid computing. Cloud computing is described as the offspring of distributed and grid computing by some authors (Che, Duan, Zhang & Fan, 2011).The straightforward meaning of cloud computing refers to the features and scenarios where total computing could be done by using someone else's network where ownership of hardware and soft resources are of external parties. In general practice, the dispersive nature of the resources that are considered to be the 'cloud' to the users are essentially in the form of distributed computing; though this is not apparent or by its definition of cloud computing, do not essentially have to be apparent to the users.

In recent years, the cloud has evolved in two broad perspectives – to rent the infrastructure in cloud, or to rent any specific service in the cloud. Where the former one deals with the hardware and software usage on the cloud, the later one is confined only with the 'soft' products or services from the cloud service and infrastructure providers. The computing world has been introduced with a number of terminologies like SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) with the evolution of cloud computing. As discussed earlier, the term 'cloud computing' is rather a concept, so are the terminologies to define different blends of cloud computing. At its core essence, cloud computing is nothing but a specialized form of grid and distributed computing which varies in terms of infrastructure, services, deployment and geographic dispersion (Hashizume et al. 2013). In a pervasive meaning within the context of computer networks, infrastructure could be thought of as the hardware as well as their alignment where platform is the operating system which acts as the platform for the software.

Thus the concept of cloud based services is hierarchically built from bottom to top in the order of IaaS, PaaS and SaaS. This is merely the level of abstraction that defines the extent to which an end-user could 'borrow' the resources ranging from infrastructure to software – the core concern of security and the fashion of computing are not affected by this level of abstraction. As a result, security is to be considered within any form of cloud computing (Bisong & Rahman, 2011) regardless of flavour, hierarchy and level of abstraction. Virtualization is an inevitable technology that is highly coupled with the concept of cloud computing – it is the virtualization technology that complements cloud services specially in the form of PaaS and SaaS where one physical infrastructure contains services or platforms to deliver a number of cloud users simultaneously. This leads to the addition of total security aspects of virtualization technology on top of the existing security concerns and issues of cloud computing. Figure 1 illustrates a typical cloud based scenario that includes the cloud service

provider and the cloud users in a cloud computing architecture.

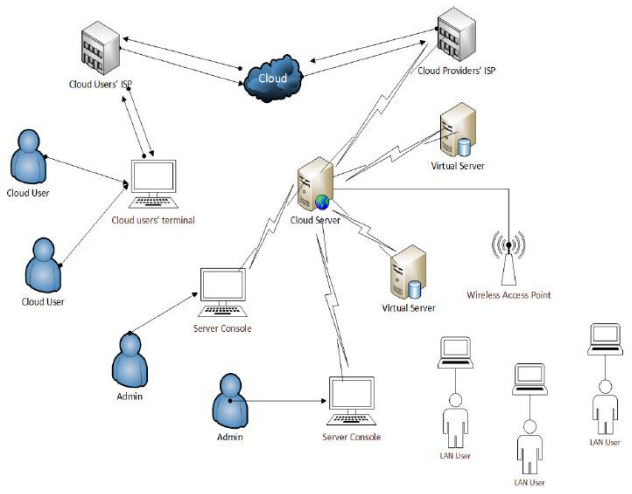

Figure 1: A Typical Cloud Architecture.

DEPLOYMENT OF CLOUD SERVICES

There are four different deployment models of cloud computing:

Public Cloud: Public or external cloud is traditional cloud computing where resources are dynamically provisioned on a fine-grained, self-service basis over the Internet or via and or from an off-site third-party provider who bills on a fine-grained basis.

Community Cloud: If several organizations have similar requirements and seek to share infrastructure to realize the benefits of cloud computing, then a community cloud can be established. This is a more expensive option as compared to public cloud as the costs are spread over fewer users as compared to a public cloud. However, this option may offer a higher level of privacy, security and/or policy compliance.

Hybrid Cloud: Hybrid Cloud means either two separate clouds joined together (public, private, internal or external) or a combination of virtualized cloud server instances used together with real physical hardware. The most correct definition of the term "Hybrid Cloud" is probably the use of physical hardware and virtualized cloud server instances together to provide a single common service. Two clouds that have been joined together are more correctly called a "combined cloud".

Private Clouds: Private clouds describe offerings that deploy cloud computing on private networks. It consists of applications or virtual machines in a company's own set of hosts. They provide the benefits of utility computing - shared hardware costs, the ability to recover from failure, and the ability to scale up or down depending upon demand.

CLOUD COMPUTING SECURITY ARCHITECTURE

Security within cloud computing is an especially worrisome issue because of the fact that the devices used to provide services do not belong to the users themselves. The users have no control of, nor any knowledge of, what could happen to their data. This is a great concern in cases when users have valuable and personal information stored in a cloud computing service. Users will not compromise their privacy so cloud computing service providers must ensure that the customers' information is safe. This, however, is becoming increasingly challenging because as security developments are made, there always seems to be someone to figure out a way to disable the security and take advantage of user information. Some of the important components of Service Provider Layer are SLA Monitor, Metering, Accounting, Resource Provisioning, Scheduler& Dispatcher, Load Balancer, Advance Resource Reservation Monitor, and Policy Management. Some of the security issues related to Service Provider Layer are Identity, Infrastructure, Privacy, Data transmission, People and Identity, Audit and Compliance, Cloud integrity and Binding Issues. Some of the important components of Virtual Machine Layer creates number of virtual machines and number of operating systems and its monitoring. Some of the security issues related to Virtual Machine Layer are VM Sprawl, VM Escape, Infrastructure, Separation between Customers, Cloud legal and Regularity issues, Identity and Access management Some of the important components of Data Center (Infrastructure) Layer contains the Servers, CPU's, memory, and storage, and is henceforth typically denoted as Infrastructure-as-a-Service (IaaS). Some of the security issues related to Data Center Layer are secure data at rest, Physical Security: Network and Server.

Some organizations have been focusing on security issues in the cloud computing. The Cloud Security Alliance is a non-profit organization formed to promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing. The Open Security Architecture (OSA) is another organizations focusing on security issues. They propose the OSA pattern, which pattern is an attempt to illustrate core cloud functions, the key roles for oversight and risk mitigation, collaboration across various internal organizations, and the controls that require additional emphasis. For example, the Certification, Accreditation, and Security Assessments series increase in importance to

ensure oversight and assurance given that the operations are being "outsourced" to another provider. System and Services Acquisition is crucial to ensure that acquisition of services is managed correctly. Contingency planning helps to ensure a clear understanding of how to respond in the event of interruptions to service delivery . The Risk Assessment controls are important to understand the risks associated with services in a business context. National Institute of Standard and Technology (NIST), USA (http://www.nist.gov/) has initiated activities to promote standards for cloud computing . To address the challenges and to enable cloud computing, several standards groups and industry consortia are developing specifications and test beds. Some of the existing standards and test bed groups are Cloud Security Alliance (CSA), Internet Engineering Task Force (IETF), Storage Networking Industry Association (SNIA) etc. On the other side, a cloud API provides either a functional interface or a management interface (or both). Cloud management has multiple aspects that can be standardized for interoperability. Some possible standards are Federated security (e.g., identity) across clouds, Metadata and data exchanges among clouds, Standardized outputs for monitoring, auditing, billing, reports and notification for cloud applications and services, Cloud-independent representation for policies and governance etc., Figure 2 showing the high level view of the cloud computing security architecture.

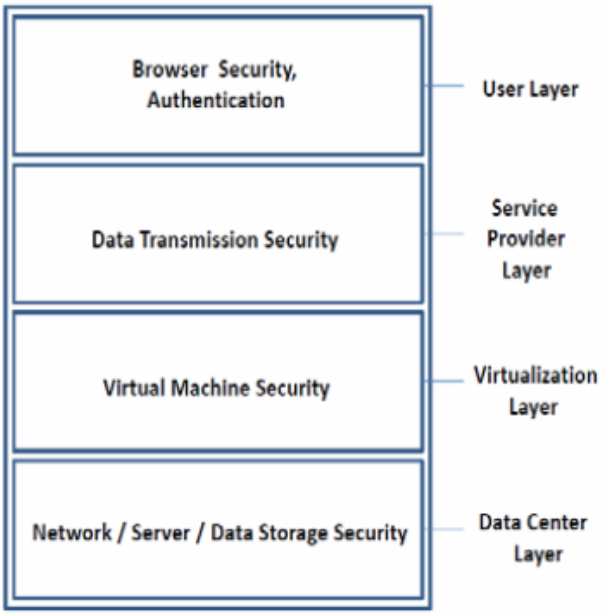

Figure 2. High Level Security Architecture of Cloud Computing.

CLOUD ENVIRONMENT ROLES

In cloud environments, individual roles can be identified similar to the typical role distribution in Service Oriented Architectures and in particular in (business oriented) Virtual Organisations. As the roles relate strongly to the individual business models it is imperative to have a clear definition of the types of roles involved in order to ensure common understanding.

(Cloud) Providers offer clouds to the customer – either via dedicated APIs (PaaS), virtual machines and / or direct access to the resources (IaaS). Note that hosts of cloud enhanced services (SaaS) are typically referred to as Service Providers, though there may be ambiguity between the terms Service Provider and Cloud Provider.

(Cloud) Resellers or Aggregators aggregate cloud platforms from cloud providers to either provide a larger resource infrastructure to their customers or to provide enhanced features (see II.B). This relates to community clouds in so far as the cloud aggregators may expose a single interface to a merged cloud infrastructure. They will match the economic benefits of global cloud infrastructures with the understanding of local customer needs by providing highly customized, enhanced offerings to local companies (especially SME's) and world-class applications in important European industry sectors. Similar to the software and consulting industry, the creation of European cloud partner ecosystems will provide significant economic opportunities in the application domain – first, by mapping emerging industry requests into innovative solutions and second by utilizing these innovative solutions by European companies in the global marketplace.

(Cloud) Adopters or (Software / Services) Vendors enhance their own services and capabilities by exploiting cloud platforms from cloud providers or cloud resellers. This enables them to e.g. provide services that scale to dynamic demands – in particular new business entries who cannot estimate the uptake / demand of their services as yet. The cloud enhanced services thus effectively become software as a service.

(Cloud) Consumers or Users make direct use of the cloud capabilities – as opposed to cloud resellers and cloud adopters, however, not to improve the services and capabilities they offer, but to make use of the direct results, i.e. either to execute complex computations or to host a flexible data set. Note that this involves in particular larger enterprises which outsource their inhouse infrastructure to reduce cost and efforts.

MOTIVATORS FOR USING CLOUD COMPUTING

Advantages of using cloud computing include:

- Pay-as-you-go pricing
- Elastic scalability
- Possibility to scale "infinitely" large
- Focus on business advantage
- "Cost associativity"

One major motivator for using cloud computing is the economic aspect and the potential savings. The pay-as-you-go model of cloud computing entails exchanging capital expenditures for operational expenditures and the economies of scale enjoyed by large corporations delivering cloud services is a potential cost saver for cloud users. The need to make investments in hardware to create a private datacenter for hosting is eliminated by the cloud model which is particularly advantageous for startups lacking the funds to make such investments.

The elasticity of cloud computing can also be a great source of monetary gain. With a private datacenter the server capacity for expected load need to be provisioned in advance since delivery, installation and configuration of new hardware takes time. Predicting future load is difficult, gives the example of a company that made its service available on Facebook and had an increase in demand from 50 servers to 3500 servers in three days.

Even though not all companies are likely to experience such surges in demand under- or over-provisioning are still risks. Over-provisioning results in unnecessary expenses for hardware that is not needed. The consequences of under-provisioning are likely even worse since insufficient capacity will result in a poor user experience that may result in a loss of customers. Failing in the provisioning of the hardware leads to these undesired scenarios but even if the prediction is correct and the hardware can handle the peak load the capacity is likely unnecessarily high the majority of the time. The load on many systems varies over the course of each day, week, or year. The load during nights, weekends, or a particular season may be lower than the average so even successfully provisioning for peak load may lead to a lot of unutilized capacity. In fact, an estimate of utilization of server capacity in datacenters puts the number at 6 % . This illustrates the benefit of being able to quickly scale up and down according to current load.

CLOUDS IN THE FUTURE INTERNET

The Future Internet covers all research and development activities dedicated to realizing tomorrow's internet, i.e. enhancing a networking infrastructure which integrates all kind of resources, usage domains etc. As such, research related to cloud technologies form a vital part of the Future Internet research agenda. Confusions regarding the aspects covered by cloud computing with respect to the Future Internet mostly arise from the broad scope of characteristics assigned to "clouds", as is the logical consequence of the re-branding boom some years ago.

So far, most cloud systems have focused on hosting applications and data on remote computers, employing in particular replication strategies to ensure availability and thus achieving a load balancing scalability. However, the conceptual model of clouds exceeds such a simple technical approach and leads to challenges not unlike the ones of the future internet, yet with slightly different focus due to the combination of concepts and goals implicit to cloud systems.

In other words, as a technological realization driven by an economic proposition, cloud infrastructures would offer capabilities that enable relevant aspects of the future internet, in particular related to scalability, reliability and adaptability. At the same time, the cloud concept addresses multiple facets of these functionalities.

CONCLUSION

Today, cloud computing is being defined and talked about across the ICT industry under different contexts and with different definitions attached to it. The core point is that cloud computing means having a server firm that can host the services for users connected to it by the network. Technology has moved in this direction because of the advancement in computing, communication and networking technologies.

Cloud computing has enormous prospects, but the security threats embedded in cloud computing approach are directly proportional to its offered advantages. Cloud computing is a great opportunity and lucrative option both to the businesses and the attackers – either parties can have their own advantages from cloud computing. The vast possibilities of cloud computing cannot be ignored solely for the security issues reason – the ongoing investigation and research for robust, consistent and integrated security models for cloud computing could be the only path of motivation. The security issues could severely affect could infrastructures. Security itself is conceptualized in cloud computing infrastructure as a distinct layer.

To summarize, the cloud provides many options for the everyday computer user as well as large and small businesses. It opens up the world of computing to a broader range of uses and increases the ease of use by

giving access through any internet connection. However, with this increased ease also come drawbacks. You have less control over who has access to your information and little to no knowledge of where it is stored. You also must be aware of the security risks of having data stored on the cloud. The cloud is a big target for malicious individuals and may have disadvantages because it can be accessed through an unsecured internet connection.

Cloud computing offers benefits for organizations and individuals. There are also privacy and security concerns. If you are considering a cloud service, you should think about how your personal information, and that of your customers, can best be protected. Carefully review the terms of service or contracts, and challenge the provider to meet your needs.

REFERENCES

- B.P. Rimal, E. Choi, and I. Lumb. A taxonomy and survey of cloud computing systems. 2009 Fifth International Joint Conference on INC, IMS, and IDC, pages 44{51, 2009.
- Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2011). Draft Cloud Computing Synopsis and Recommendations. National Institute of Standards and Technology (NIST) Special Publication 800-146. US Department of Commerce. May 2011.
- Catteddu, D; Hogben, G eds. (2009), 'Cloud Computing - Benefits, risks and recommendations for information security', European Network and Information Security Agency (ENISA)
- Che, J. Duan, Y, Zhang, T. and Fan, J. ().Study on the security models and strategies of cloud computing. Procedia Engineering, 23, 586 – 593. doi:10.1016/j.proeng.2011.11.2551
- Hashizume et al. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(5), 1-13.
- J.L. Y. Z. Jian Wang, "A New Privacy Preserving Approach used in Cloud Computing" pp. pp. 439-440, 2010.
- Lewis, Grace. Basics About Cloud Computing (2010).
- Ogigau-Neamtiu, F. (2012). Cloud Computing Security Issues. Journal of Defense Resource Management, 3(2), 141-148.
- Petre, R. (2012). Data mining in Cloud Computing. Database Systems Journal, 3(3), 67-71.
- Singh, S. and Jangwal, T. (2012). Cost breakdown of Public Cloud Computing and Private Cloud Computing and Security Issues. International Journal of Computer Science & Information Technology, 4(2), 17-31.
- Vaquero, L. M.; Rodero-Merino, L.; Caceres, J. & Lindner, M. (2009), 'A break in the clouds: towards a cloud definition', SIGCOMM Comput. Commun. Rev. 39(1), 50--55.