International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 8, October - 2012

Cloud – The Next Phase Of Future Computing

Vivek Bhushan[1]
Department of Computer Science Engineering
Noida, India

Aarti Khetan[2]
Department of Computer Science Engineering
Noida, India

***Abstract* - Cloud Computing has been one of the most driving and fastest-growing computing technology in information technology (IT) processes and marketplace since last few years. It has achieved a top buzzword status due to its cost saving, high availability and easy scalability features. The main advantage of cloud is that it can store and transmit a huge amount of data as services via Internet. Despite of the increasing popularity in cloud computing, it has many security and privacy issues like privileged user access, regulatory compliance, data location, data segregation, recovery etc.,. This paper discuss the noble survey on cloud computing where the basic concept, phases of computing paradigm, applications, challenges and security issues, security management standards, attacks of cloud computing has been discussed.**

Keywords – cloud computing; phases; challenges; security issues; security management standards; attacks

I. INTRODUCTION

Cloud computing is the newly evolved stage which is an extension of grid, virtualization, Web2.0, Service Oriented Architecture (SOA) technologies and their convergence in the Internet. It is called the Sixth Generation of Computing (after Mainframe, Personal Computer, Network Computing, Internet Computing, and Grid Computing Computing). It provides its services via Internet on a *pay-as-you-go* service. The term cloud in cloud computing defines the way in which every service can be serviced to the customer whenever required. Resources can be accessed from the cloud whenever required and from any location over Internet. Cloud has the great feature of *elasticity* means services can be easily expanded and contracted depending upon the situation and this elasticity features is responsible for moving individuals, business and IT users towards cloud.

In 2011, National Institute of Standards and Technology (NIST) provided the proper definition[1] of cloud computing as "*Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources(software and hardware) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models".*

The main thing in cloud computing is that consumer only use, what they need, and pay for what they actually use. Clients do not worry about the maintenance of systems in the cloud. This is why, cloud computing is also called *"Utility computing"* or "*IT on demand*" [2].A simple diagrammatic cloud can be shown in fig 1.1.

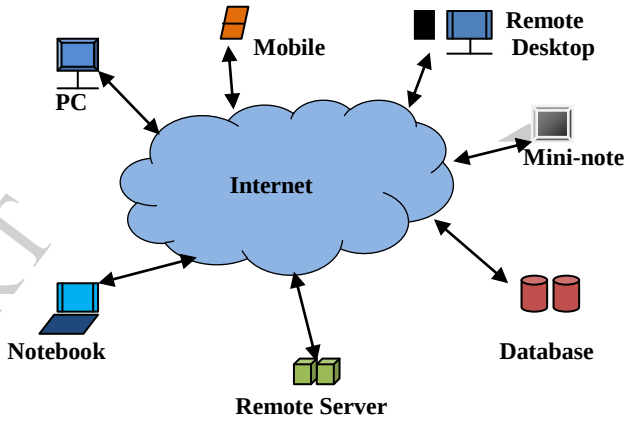

Fig. 1.1 Cloud Computing Technology

In cloud computing, a user can use a range of devices like PC's, laptops, notebooks, database, remote server, mobile phones, and PDAs to access the resources over the Internet.

Cloud computing is the fastest-growing segment within the IT Outsourcing (ITO) market and is expected to grow 48.7 percent in 2012 to $5.0 billion, up from $3.4 billion in 2011 (Gartner- Gartner Newsroom, 2012) [3].

International Data Corporation (IDC-2012) says that the cloud computing has a compound annual growth rate (CAGR) of 27.6% [4] and by 2015, one of every seven dollars spent on packaged software will be through the public cloud model.

Table I
Cloud Spending up to 2012

Year	2008	2012	Growth
Cloud IT Spending	$16B	$42B	27%
Total IT Spending	$383B	$494B	7%
Total - Cloud Spend	$367B	$452B	4%
Cloud / (Total-Cloud) Spend	4%	9%	

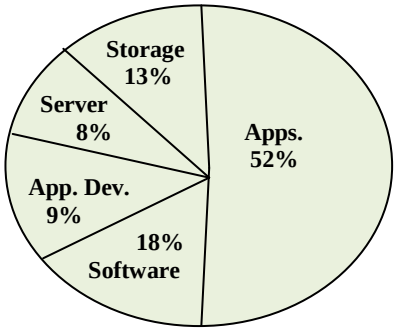

Fig. 1.2 Worldwide Distribution of Cloud in 2012

The worldwide distribution of cloud computing can be divided into five categories – *applications, software, storage, application development* and *server* and this has been represented as in the figure 1.3.

In cloud computing there are two actors called front end and back end [5] which are connected through Internet. The front end is the user who use the service provided by the back end which is the cloud section of the system.

A. Phases of Computing Paradigm

According to Voas and Zhang (2009) [6] there are six phases of computing paradigms shown in fig.1.4.

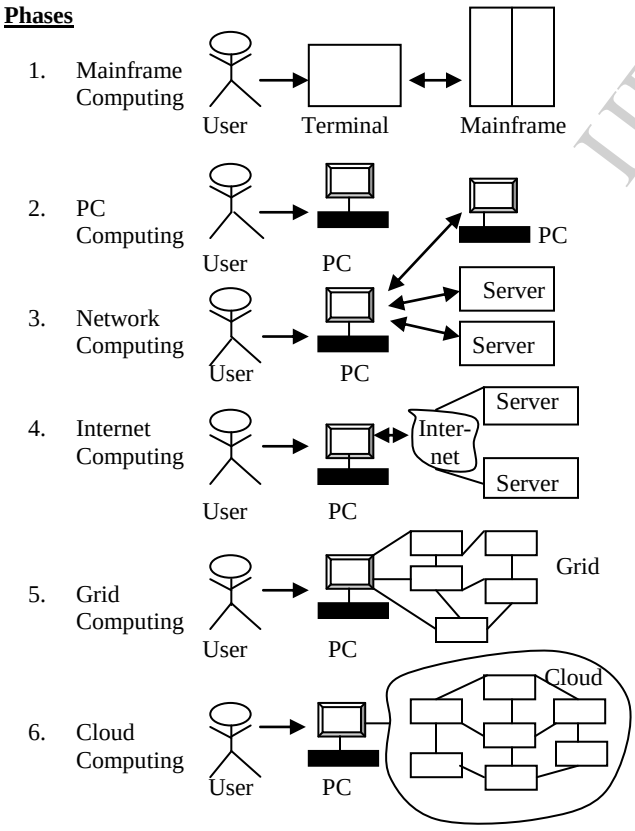

Fig. 1.3 Six computing paradigms – from mainframe computing Internet computing, to grid computing and cloud computing.

In *phase 1*, powerful mainframe was shared among many users through dummy terminals. In *phase 2*, stand-alone PCs became one of the powerful machines to provide users the maximum resources. In *phase 3*, devices like laptops, PCs and servers were connected together via local area network (LAN) to form a global network and increase throughput. In *phase 4*, the remote applications and resources were utilized by connecting different local area networks through a global network (internet). In *phase 5*, distributed computing system was developed by grid computing which provided shared computing power and storage. In *phase 6*, the concept of cloud computing evolved providing shared resources on the Internet in an easy and scalable way.

When these six paradigms are compared, it can be said that the cloud computing provides an infinite power and storage capacity than the mainframe computing which offers a limited computing power. Also, in cloud computing, the powerful PCs can support both local computing power and caching while in mainframe the dummy terminals were used as user interface devices.

II. APPLICATIONS OF CLOUD COMPUTING

Cloud computing offers a range of services through distributed cloud model. Some of the most popular cloud-based IT solutions [2] are listed below.

1. *Hosted Desktops*

With hosted desktops there is no need of traditional desktops and hence it reduces the cost of needed service. A hosted desktop is similar to regular desktops PC, but the software and data which are used by the customer are placed in remote, highly secure data centers, rather than on their own machines. Hosted desktops can be accessed from anywhere in the world via Internet connection using a specialized device called a thin client.

2. *Hosted Email*

Hosted Microsoft Exchange® email plans are taking the attention of most of the organizations which need a secured and reliable email solution with minimum expenditure. This hosted email platform helps small as well as large businesses because these businesses are not required to invest in the costly infrastructure. Emails are stored on managed servers which provide redundancy as well as quick connectivity from any location. It also helps users to access their email, calendar, contacts and shared files using a range of tools like Outlook®, Outlook Mobile Access (OMA) and Outlook Web Access (OWA).

3. *Hosted Telephony (VOIP)*

VOIP is just '*Voice Over IP*', by which phone calls and services in digital networks are carried out. It is no more different than the traditional telephony but the main feature is cost advantages. A hosted VOIP system is pre-configured handsets which just need to be plugged into

the broadband. So, the cost of investing in expensive phone system, installation, handsets, BT lines etc. can be saved. With hosted VOIP users can access voicemail, IVR and much more features.

4. *Cloud Storage*

The demand of cloud storage is growing day-by- day due to its features like simplicity, Capital Expenditure(CapEx), free costs, anywhere access and no burden of in-house maintenance and management. It is just the service in the form of delivering data storage from a third party provider. The billing is calculated on the basis of the capacity used in a certain period (e.g. per month).

5. *Dynamic Servers*

The next generation of server environment is dynamic servers with the aim of replacing traditional dedicated servers. For example the provider like ThinkGrid provides its customer access to those resources which look and feel almost like a dedicated server with the features of scalability. User have the full control on amount of processing power and space being used, so the users do not need to pay for the hardware which are not needed. The user is free to make changes to the dynamic server at any time.

III. CHALLENGES AND SECURITY ISSUES OF CLOUD COMPUTING

The Internet "cloud" has been the host topic in the world of computing, but the trend has created a new range of security issues which must be addressed.

With the rapid growth in cloud computing, the cloud security concerns also increases since it includes many technologies like networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. In the current time we cannot find the security enhancement compared to the growth of a large number of products of cloud computing.

The organization where cloud security is the primary concern continues to hesitate to transfer their business to cloud. Security issues has become one of the top-most barrier of the development and widespread use of cloud computing. Because the data is stored in the cloud, the hacker may try to get that important data.

A. Challenges of Cloud Computing

There are three main challenges for creating a trustworthy and secure cloud system [7] namely *outsourcing*, *multi-tenancy* and *massive data and intense computation.*

1. *Outsourcing*

Outsourcing has two benefits - reduce capital expenditure and operational expenditure. But outsourcing also means that the physically the customers lose control on their data and tasks. So, this loss is one of the biggest threat in cloud insecurity. The problem of outsourcing can be solved in two steps. First, the cloud provider must provide trust in secure computing and data storage in order to make themselves trustworthy. Secondly, the outsourced data and computation must be verifiable to customers in the terms of confidentiality, integrity, and other security services. Also, the outsourcing indulges in privacy violations because the classified data is out of owner's control.

2. *Multi-tenancy*

Multi-tenancy means that the cloud platform is shared and multiple customers can utilize that platform. However, in a virtualized environment, data belonging to different customers may be placed on the same physical machine using certain resource allocation policy. So, a legitimate cloud customer may exploit the co-residence issue. A series of security issues such as data breaches [8], [9], [10], computation breach [11], flooding attack [12], etc., are incurred. Multi-tenancy leads to new vulnerabilities in the cloud platform. Without changing the multi-tenancy paradigm, it is not possible to design such security technologies which can deal with the potential risks.

3. *Massive data and intense computation*

Cloud computing is known for its capacity to store and handle mass data and intense computing tasks. So, the traditional security mechanisms are not sufficient enough to handle such huge data due to the unbearable computation or communication overhead. Data integrity proofs become important issue when data is remotely stored. So, new strategies and protocols are expected to be built in order to handle such situations.

B. Supporting Techniques

Cloud computing has leveraged a list of techniques like Data Center Networking (DCN), Virtualization, distributed storage, MapReduce, web applications and services etc.

1. **Modern data center** has been an effective carrier of cloud computing environments. It provides huge computation and storage capability by composing thousands of machines with DCN techniques.
2. **Virtualization** is the widely used technology in cloud computing to provide dynamic resource allocation and service provisioning, especially in IaaS. Virtualization has the benefit of running more than one operating system on the same machine without considering about their hardware platforms.
3. **MapReduce [13]** is a programming framework given by Google for processing large data sets especially distributed computing on clusters of computers. This breaks large data sets into small blocks which are distributed to cloud servers for parallel computing. MapReduce speeds up the batch processing on

massive data and thus it helps the cloud vendors to select it as a computation model.

C. Security Issues in Cloud Computing

As it is discussed that cloud computing is the sixth phase of computing paradigm, but at the same time the vulnerabilities also keep on growing on a large scale which leads to several threats. According to the survey conducted by IDC on 244 IT executives/CIOs, security ranked first as the greatest challenge or issue of cloud computing [14], shown in fig. 1.11.

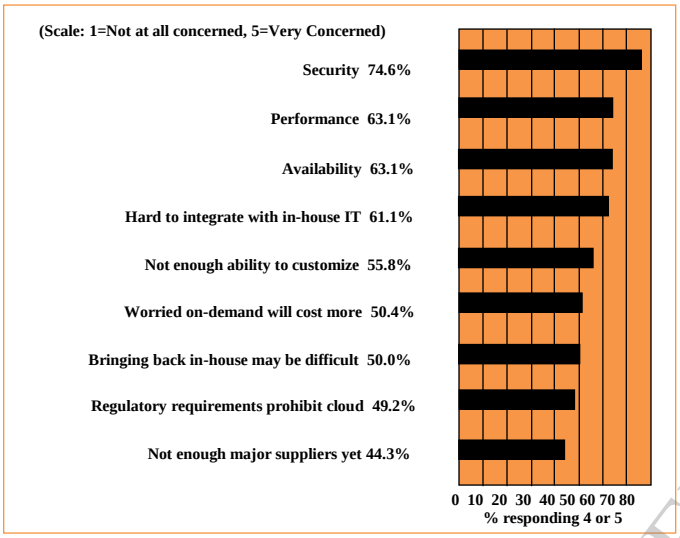

Fig. 1.9 Result of IDC survey ranking security challenges

Cloud computing has strong Government support and promotion in Europe, the United States and other countries. Also the Government has taken attention on the issues of cloud computing. In November, 2010, the U.S. Government CIO council published the Government document that the Government agencies use cloud computing, which described the challenges of cloud computing and security for cloud computing, asked various institutions to assess the security risks, which can be compared with their security needs. Their analysis shows that unified risk assessment and authorization identified by the Government authority institution can accelerate the assessment and the use of cloud computing and reduce the cost of risk assessment.

There are seven main security issues [15] of cloud computing described below.

1. Privileged user access

Since the information is transmitted from the customers via the Internet, it creates some level of risk. So, an enterprise must test their service provider that all the regulations are fully satisfied and the SLAs are maintained.

2. Regulatory compliance

As there are a large number of service providers, clients can choose any provider. But a client must ensure that the level of data integrity and security are maintained by that provider but it still remains a problem.

3. Data location

Depending on contracts, some clients might never know that in which country or under what jurisdiction their data is located. So, the issue of data loss still remains.

4. Data segregation

In cloud, there is a huge data from various companies in the encrypted form. So, there must be a solution to categorize the data.

5. Recovery

Every provider should have a disaster recovery protocol to protect user data in the case if all the data is lost by any customer or provider.

6. Investigative support

If a client suspects faulty activity from the provider, he/she may have many legal ways to investigate it and proper channels to communicate also.

7. Long-term viability

A client must be able to stick on their contract even if their current provider is undertaken by any other enterprise.

8. Safety standards

There must be worldwide acceptable standard in order to ensure confidentiality, integrity and availability.

9. Network attacks

Presently the network attack is the biggest challenge of network security. Since there is continuous increase in the migration of data of customers, organizations and packages, the more chances of networks attacks and frauds. According to the security experts, cloud computing will be the focus of hackers in the coming next five years.

D. Security Management Standards

There are three standards that are related to security management practices in the cloud namely *Information Technology Infrastructure Library (ITIL), International Organization for Standardization (ISO) 27001/27002* and *Open Virtualization Format (OVF).*

1. Information Technology Infrastructure Library (ITIL)

The main purpose of ITIL is to ensure that the right approaches in security must be taken so as to handle the levels of security. In ITIL, the information is

broken down into process, policy, procedure, and work instruction.

2. ***International Organization for Standardization (ISO) 27001/27002***
   ISO 27001 defines the mandatory requirements for an Information Security Management System (ISMS). It is also a certification standard and uses ISO 27002 to indicate suitable information security controls within the ISMS.

3. ***Open Virtualization Format (OVF)***
   It enables efficient, flexible, and secure distribution of enterprise of software, facilitating the mobility of virtual machines and giving customers and vendors platform independence. Clients must be able to deploy an OVF formatted virtual machine on any virtualization platform..

E. Cloud Computing Attacks

Since more and more companies are moving to cloud computing, it gives hackers a lot of chance to exploit their data. Some of the potential attack vendors criminals may attempt include-

1. ***Denial of Service (DOS) attacks***
   According to security professionals, since cloud is shared by many users, so it is more prone to DoS attacks. In a survey, it is already shown that in year 2009, Twitter was the victim of DoS attacks.

2. ***Side Channel attacks***
   A clever attacker can easily deploy a malicious virtual machine near a victim‘s server and then perform the attacks in the form of side channel attack.

3. ***Authentication attacks***
   It is the most strong point for attacking a virtual machine because there are various techniques of authenticating a user such as a name of the user.

4. ***Man-in-the-middle cryptographic attacks***
   An attacker may be placed between two clients. Anytime attackers can place themselves in the communication path, there is the possibility that they can intercept and modify communications.

IV. CONCLUSION

Throughout this paper we have shown that cloud computing has a bright future due to its several exciting features like on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service, lower cost, ease of utilization, quality of service, reliability, simplified maintenance and upgrades, outsourced IT management and low barrier to entry. There are various benefits and applications of cloud computing like hosted desktops, hosted email, dynamic servers, hosted telephony and cloud storage. Besides the benefits of cloud computing, there are several challenges like outsourcing, multi-tenancy, and massive data and intense computation. Further, cloud computing faces several security issues like regulatory compliance, data location, data segregation etc. which creates the barrier for the development of cloud computing. The security management standards ITIL, ISO 27001/27002, and OVF must be followed so as to have a bright future of cloud computing.

REFERENCES

[1] Final Version of NIST Cloud computing Definition Published, 2011.www.nist.gov/itl/csd/cloud-102511.cfm
[2] Albion: Cloud Computing-Opportunities and challenges for SMEs 2011. www.albion2000.com
[3] Gartner NewsRoom – Worldwide IT Outsourcing Services Spending, 2012. http://www.gartner.com/it/page.jsp?id=2108715
[4] IDC: IDC Cloud Research, 2012. http://www.idc.com/prodserv/idc_cloud.jsp
[5] Wentao Liu, “Research on Cloud Computing Security Problem and Strategy” ,2011.
[6] Furht, Borko, Handbook of Cloud Computing, Armando, Springer, 2010.
[7] Xiao and Xiao, “Security and Privacy in Cloud Computing”, IEEE, 2012.
[8] Google Docs experiences data breach during March 2009. http://blogs.wsj.com/digits/2009/03/08/1214/
[9] S. Savage & T. Ristenpart, “Hey, you, get off My cloud: exploring information leakage in third-party compute clouds”,M. 2009.
[10] N. Santos, R. Rodrigues, “Towards Trusted Cloud Computing”, 2009.
[11] C. Dovrolis and D. Moore, “What do packet dispersion technique Measure?”, IEEE Infocom, 2001.
[12] Cloud Security Alliance (CSA) “ Top Threats to Cloud Computing”, M.2010.
[13] A.Charlesworth, S. Pearson, “Mapreduce: Simplified Data Processing On Large Clusters”, USENIX Association, USA, O.2008.
[14] International Data Corporation (IDC) http://blogd.idc.com/ie/wpcontent/uploads/2009/12/idc_cloud_challenges_2009.jpg, 2009.
[15] GartnerNewsRoom,2011, “Security Issues in Cloud Computing” http://www.gartner.com/technology/research/security-risk-management/cloud-security.jsp