International Journal of Engineering Research & Technology (IJERT)
NCAEM-2013 Conference Proceedings
ISBN: 978-93-83758-09-8

Security Risks and Future of Cloud Computing

[1]Meetu Galhotra, [2]Divya Malhotra
[1,2]M.Tech Student, Geeta Engineering College
Panipat (Haryana)
[1]meetu023@gmail.com, [2]divya.malhotra19@gmail.com

***Abstract*: The concept of cloud computing represents a shift in thought, in that an end user needs not to know the details of technology. The service is fully managed by the provider. The cloud is a next generation platform that provides dynamic resource pools, virtualization, and high availability. This paper represent clear description of with different characteristics of cloud computing. Customers are also very concerned about the risks of Cloud. They always worry about Security. The purpose of this document is to describe different security threats.**

***Keywords*: Cloud Computing, Security, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)**

I. INTRODUCTION

Cloud computing is a technology that uses the internet and to maintain data and applications. Cloud computing allows consumers to use applications without installation and access their personal files at any computer with internet access. A simple example of cloud computing is Yahoo email, Gmail, or Hotmail etc. You don't need a software or a server to use them. All a consumer would need is just an internet connection. The server and email management software is all on the cloud (internet) and is totally managed by the cloud service provider Yahoo, Google etc. Cloud computing is cheaper than other computing models no maintenance cost is involved because service provider is responsible for the availability of services. Cloud computing can be described in three segments: "application" "storage" and "connectivity". Each segment serves a different purpose and offers different products for businesses and individuals around the world.

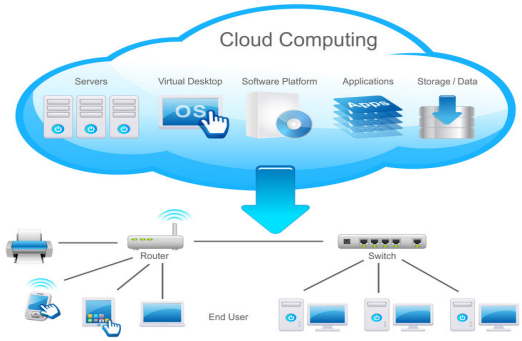

Fig 1. General working of cloud computing

II. ARCHITECTURE

The architecture of Cloud computing can be categorized according to the three types of delivery models, namely Infrastructure as a service (IaaS), Software as a service (SaaS) and Platform as a service (PaaS).

A. Infrastructure as a Service (IaaS)

Infrastructure as a Service is a single tenant cloud layer where the Cloud computing vendor's dedicated resources are only shared with contracted clients at a pay-per-use fee. This greatly minimizes the need for huge initial investment in computing hardware such as servers, networking devices and processing power.

B. Software as a Service (SaaS)

Software as a service is where computer applications are accessed over the Internet. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support Web services and service-oriented architecture (SOA). Information security officers will need to consider various methods of securing SaaS applications. Web Services (WS) security, Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL) and available options which are used in enforcing data protection transmitted over the Internet.

C. Platform as a Service (PaaS)

Platform as a service cloud layer works like IaaS but it provides an additional level of "rented" functionality.

III. CHARACTERISTICS OF CLOUD COMPUTING

A. Dynamic Scalability

A key benefit of cloud computing is the ability to add and remove capacity as and when it is required. This is also known as elasticity. Cloud computing is **dynamically scalable** because users only have to utilize the amount of online computing resources they actually required.

B. Cloud computing is task-centric

Cloud computing is task centric because it totally depends on the task the user wants to achieved and not on particular software, hardware or network infrastructure.

ISBN: 978-93-83758-09-8

Users do not have to purchase or install anything before using a cloud computing resource.

C. Cloud computing is independent of devices used

Device Independence in the context of cloud computing means the freedom or power of cloud users to access their data or files in different devices or gadgets whether it is mobile phone, personal computer or any similar gadgets . It is very simple and practical to make possible for users to access applications and information located in the cloud systems in spite of their place or what tool or machine they are utilizing.

D. Resources reuse, low cost

As cloud computing adopts statistical multiplexing technology of resources, IT physical resources are increasingly used in a large scale, thus, the cost of cloud business is greatly reduced.

E. Service-oriented

Cloud computing systems are all service oriented - i.e. the systems are such that they are created out of other different services. Many such cloud computing different individual services combine together to form this service. Other such services can be created by using services that were just created. There are two keys to achieve the service oriented conception i.e. abstraction and accessibility.

F. Cloud computing is programmable

Many necessary task of cloud computing must be automated. for e.g., to protect the integrity of the data, information stored on a single computer in the cloud must be copied on another computer in the cloud . If that computer goes offline, the clouds programming automatically redistributes that computer's data to a new computer in the cloud.

IV. SECURITY IN CLOUD COMPUTING

According to CIO Research Center Report Security continues to be the biggest concern for CIOs when looking at Cloud adoption.

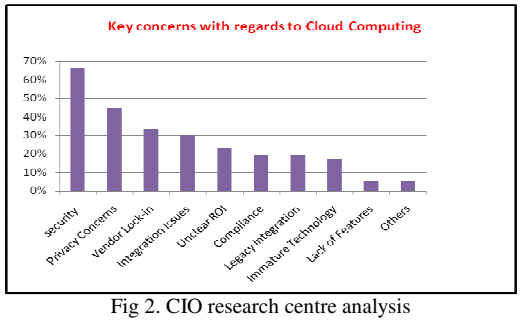

Fig 2. CIO research centre analysis

Following are the security threats encountered in cloud computing:

A. Denial of service attack

The aim of a denial of service attack is to deny legitimate users access to a particular resource

When the high workload on the flooded services notifies by Cloud Computing operating system then it will start providing more computational power to cope with the additional workload. Thus, the server hardware boundaries for maximum workload to process do no longer hold. In that sense, the Cloud system is trying to work against the attacker,but in some extent this will help by enabling him to do most possible damage on a service's availability, starting from a single flooding attack entry point. Thus, the attacker does not have to flood all n servers that provide a certain service in target, but merely can flood a single, Cloud based address in order to perform a full loss of availability on the intended service.

B. Man-in-the-middle attack

The man-in-the-middle attack (often abbreviated MITM). As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. It is also defined as active eavesdropping where attacker makes independent connections between users and relays messages between them. Man-in-the-Middle attacks are often referred to as "session hijacking attacks", in which the intruder aims to gain access to a legitimate user's session.

C. Network Sniffing

A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. Data packets are transmitted from one network device to another which causes the risk that outsider could see our data. Sniffing is used to see what type of traffic is being passed on a network and to look for things like passwords, credit card numbers, and so forth.

D. Port Scanning

Port scanning can be defined as 'doors,' through which intruders gain access to computers". The basic step is simply sends out a request to connect the target host on each port sequentially. It is the technique used to identify open ports and services available on a network host but it also used by hackers to target victims. If repetitive port scans are made, a denial of service can be created. Hackers typically utilize port scanning because they can easily identify services which can be broken. They

ISBN: 978-93-83758-09-8

conduct tests for open ports on Personal Computers that are connected to the web.

E. SQL Injection Attack

There is a big influence of web application on our life. Several business houses and governments and society in general depend on this. All these web applications are accessed via internet therefore security risks associated with it. Usually RDBMS (Relational Database Management Systems) is used for database by web applications . They provide interface to the user to input the information in the form of SQL statements which are executed on the RDBMS. By using SQL injection, malicious user can alter the protected data, leak the sensitive information or crash the entire system.

F. XML Signature Element Wrapping

In cloud computing, clients are connected via a web browser or web service which increases the probability of web services attacks in cloud computing. XML signature element wrapping is common attack for Web service. XML sign are designed to facilitate integrity protection and origin authentication for a variety of documents types. It is use to defend a component name, attribute and value from illegal party but unable to protect the position in the documents. An attacker is able to manipulate a SOAP message by copying the target element and inserting whatever value the attacker would like and moving the original element to somewhere else on the SOAP message. Suppose we use a signature to secure the transmit data then outsider can't be able to change that data. But this attack allows a malicious user to change the signed information what is being sent.

G. Browser Security

In a cloud computing system, the computational processes are completed in the cloud server whereas the client side just send a request and wait for the result. Web browser is a common method to connect to the cloud systems. Before a client can request for services on the cloud system, the client is required to authenticate himself whether he has an authority to use the cloud system or not. As a client sent the request to the server by web browser the web browser have to make use of SSL to encrypt the credentials to authenticate the user . But SSL support point to point communication means the attacker may get the credentials of the user and use in these credentials in the cloud system as a valid user by installing sniffing packages on intermediary host.

H. Cloud Malware Injection Attack

Cloud malware injection attack is to make attempt to inject a malicious service, application or even virtual machine into the cloud system depending on the cloud service models (SaaS, PaaS and IssA) In order to perform this attack , the first step of intruder is to generate his personal vindictive application[3]. Once the vindictive software is entered into the cloud structure the attacker had to trick the cloud system to treat the malicious software as a valid instance. If successful user ask for the vindictive service then malicious is implemented. Attacker can also upload virus program in to the cloud system. Once the cloud system treats it as a valid service, the virus program is automatically executed and the cloud system infects the virus which can cause damage to the cloud system.

J. *Incomplete Data Deletion*

In cloud computing, replica's of data is placed in over different server because of this data does not remove completely. This is known as Incomplete Data Deletion. When a request to delete a cloud resource is made, most operating systems this will not remove accurately Accurate data deletion is not possible because copies of data are stored on another sever but are not available.

Denial of Service:	***Reduction of the privileges of the user that connected to a server.***
Man in the Middle Attack	Proper installation of SSL
Network Sniffing:	Use of encryption methods for securing the data.
Port Scanning:	Use of firewall to secure the data from port attacks.
SQL Injection Attack:	Web applications should not use one connection for all transactions to the database
Flooding Attacks	Intrusion detection system will filter the malicious requests and installing firewall.
XML Signature Element Wrapping:	Careful security policy specification and correct implementation by signed message providers and consumers.
Browser Security:	Use of WS-security concept on web browsers by vendors.
Cloud Malware Injection Attack	Authenticity check for received messages is required.
Flooding Attacks	Installation of a firewall or intrusion detection system (IDS)
Incomplete Data Deletion	Use of virtualized private networks for securing the data

Table 1: Different security threats and their countermeasures

V. CLOUD COMPUTING SURVEY IN INDIA

According to a survey of Google Trends, the term cloud computing became popular in 2007. The Fig 3 shows the growth of the Cloud computing around the world from

ISBN: 978-93-83758-09-8

2009 to 2013. Trends of searching information concerning cloud computing is increased exponentially over the last four years.

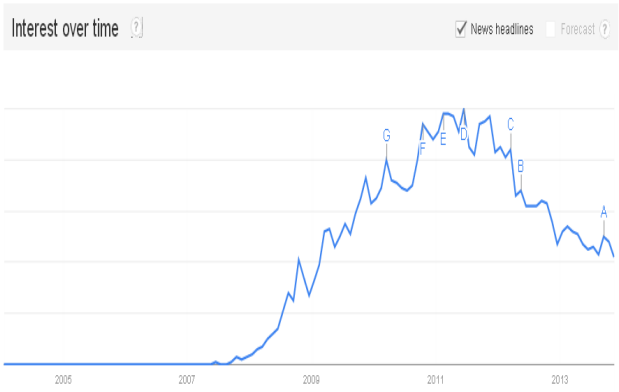

Fig.3: Searches for cloud computing from worldwide on google.com, taken from Google Trends.

Progress of Cloud Computing in India is faster than other countries. According to a survey, a list of top 10 countries ranked in surfing cloud computing, this is shown in the Fig 2.

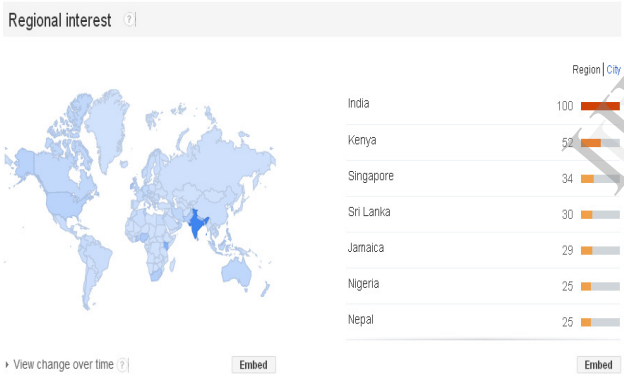

Fig.4: Searching Trends of Cloud Computing by different countries, taken from Google Trends

Cloud computing, which has existed in some form or the other since 2005 but only picked up over the last three years, is a new paradigm whereby computing is delivered as a service over the Internet rather than as a product installed inside a company's premises.

Gartner estimated that SaaS market in India was US$27 million in 2007. According to a study by Springboard Research, the Indian SaaS market would experience a CAGR (compound annual growth rate) of 77% during 2006-2010 and will reach US$165 million in 2010 (IANS 2008). According to a study by India's National Association of Software and Services Companies (*NASSCOM*) and Mckinsey, remote infrastructure management will be a US$15 billion industry in India by 2013.

Cloud computing is growing in India and according to a study conducted by Nasscom and Deloitte last year, predicted the market to clock revenues of $16 billion by 2020. Mr Floris van Heist, General Manager, Business and marketing, Microsoft Corporation India, said The IT/ITeS sector has been in the forefront of job creation and in FY11, employment in the IT/BPO sector reached 2.5 million with an addition of 2.4 lakh employees and indirect job creation was estimated at 8.3 million.

VI. CONCLUSION

In Cloud computing software applications, processing power, data and even artificial intelligence are accessed over the Internet. We do not experience maintenance issues and operating system expenses whereas all these issues are encounter in traditional servers. But Cloud computing if not properly secure. This paper discusses many security threats along with their countermeasures. There is great need of adopting more secure strategies to make the cloud structure secure in all aspects. Despite of security risks, cloud computing gets positive response in India. Finally, the paper presents an figure which shows that there will be boom of jobs in this field in coming years.

REFERENCES

[1] Cynthia Bailey Lee , Chris Roedel, Elena Silenok "Detection and Characterization of Port Scan Attacks".
[2] Cloud Confusion Amongst IT Professionals. Version One (June 6, 2011).
[3] Danish Jamil, Hassan Zaki "Security Issues In Cloud Computing And Countermeasures", International Journal of Engineering Science and Technology (IJEST).
[4] http://explainingcomputers.com/cloud.html
[5] Farhan Bashir Shaikh, Sajjad Haider "Security Threats in Cloud Computing",6th International Conference on Internet Technology and secured Transaction,UAE
[6] Google Trends search analysis for cloud computing, http://www.google.com/trends?q=cloud+computing, retrieved on July 2011.
[7] Google Trends search analysis for cloud computing in India,http://www.google.com/trends?q=cloud+computing&ctab=0&geo=in&date=all&sort=0, retrievedon July 2011. [8] ISO 7498-2:1989. Information processing systems- Open Systems Interconnection. ISO 7498-2