IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

An Investigation towards Security Threats for Cloud Computing

Santanu Kumar Sen[*1], Sharmistha Dey[2]

[*1,2]Gurunanak Institute of Technology, Sodepur, Kolkata, India

profsantanu.sen@gmail.com

Abstract

Cloud computing, a disruptive technology of the recent era, is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources having its intrinsic potentiality to enhance collaboration, agility, scaling, 24x7 availability with immense opportunity for cost reduction through optimized and efficient computing. Its tremendous envision capability to cater components rapidly orchestrated, provisioned, implemented and decommissioned, scaling and on-demand utility-like model of allocation and consumption, is however, not free from some serious drawbacks due to its inherent security breach. The information security in cloud, which is comprised of network security and data security as well, has become a major challenge for the cloud developers and providers because of the problem of hacking and attack vectors launched by malicious users or intruders.

A good number of attack vectors and threats have been identified responsible for the decline of the widespread of the cloud computing in the IT and ITes industries and a major thrust research area has been evolved in the current decade, particularly, to device and formalize the appropriate security metrics for the measurement of the impact of the varied attack vectors.

This paper focuses on several attack vectors commonly encountered in the particular area of cloud security making the technology vulnerable and unpopular. As nobody in the industries or academia is willing to compromise with privacy and security whatever advantageous the technology is, cloud computing, being a value added service, with all its virtue, is facing a great challenge to the cloud service providers and users.

Keywords: DDOS Attack, VM-Virtual machine, Risk factor, Weight Factor, TA Index, ROTA.

Introduction

Cloud computing is one of the most robust and popular technology adapted by industries showing the way to increase the capacity or add capabilities dynamically, without investing any new infrastructure. NIST (National Institute of Standards and Technology), USA, provides the most accepted definition for cloud computing. “Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [1]. The name “cloud” came from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. The cloud symbol was used to represent the Internet as early as 1994.The core concept of cloud computing comes around the year of 2004-2005. In the year 2006, when Amazon Web service (AWS) was first launched on a utility computing basis, the essence of cloud computing started for the industry. The idea of an "intergalactic computer network" was introduced in the sixties by J.C.R. Licklider, who was responsible for enabling the development of ARPANET in 1969 [2].

The agility, multi tenancy, virtualization and better performance of a cloud have made this technology enormously growing with the time. With traditional ‘off-the-shelf’ software packages, an application is normally installed on the company's main server, and then on each computer in the office.

Although, cloud computing have been for decades, but of late, its inevitability in the industries ranging from medium to large and service to manufacturing could have been realized. That the recent IT industry could not survive without cloud is well sensed because of its wide adoptability and applicability not only to the hardware and software services over the internet, but also, for its embracement of multitude and multi-dimensional service capabilities ranging from mature sales force management to email and photo editing to the latest smart phone applications and the entire social networking phenomenon, to mention a few. The only major apprehension of its unacceptability in the real-life applications is because of its weakness on

privacy and security issues, which is obviously, a big concern for both for providers and users. With the improvement of technologies, the attackers or hackers are able to launch attack vectors over cloud services causing a headache to the service providers and users as well [3].

Instead of so many clear benefits in the emerging cloud technology, however, the field is not picking up the pace as it should be and this is mainly because of the privacy and security issues lying intrinsically in the technology itself. Cloud computing, being a value added service, security has become a major concern for the cloud developers and also for cloud users [4].

Cloud security is an evolving sub-domain under the arena of information security that consists of network security, data security and also the computer security as a whole. The major security threat for cloud computing are several attack vectors, which cause great impacts on cloud services, that includes viruses, e-mail attachments, Web pages, pop-up windows, instant messages, chat rooms and deception. In brief, due to some popular as well as comparatively uncommon attack vectors, the security of cloud service has arose a big question in the success of the technology, which is very essential to measure properly to ensure the loss caused and also for adapting the appropriate countermeasures for those attacks. Thus, the area of privacy and security in cloud environment has emerged as a powerful research area, which has been under consideration and strict observation by several cloud researchers [5]

Threats are generally much easier to list than to describe, and much easier to describe than to measure. As a result, many organizations list threats, fewer describe them in useful terms and fewer measure them in meaningful ways. It has been observed that any system could be continuously monitored for several attack vectors and steps could be taken to control those attacks with appropriate measures.

The domain of the problem is chosen in the cloud security area because of its novelty, importance, wide scope of research, applicability in the real-life industries and also the carry forward prospect in the relevant field for future research works.

Architecture of Cloud

From an architectural perspective, shown in Figure 1, there is much confusion surrounding how cloud is both similar to and different from existing models of computing and how these similarities and differences impact the organizational, operational, and technological approaches to network and information security practices [2][6].

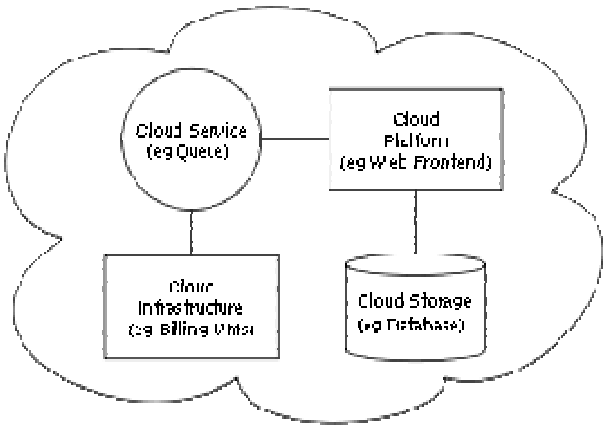

Fig. 1

A. Types of Clouds

There are basically three main types of clouds, viz., Public Cloud, Private Cloud and Hybrid Cloud. However, there are some special purpose clouds commercially used in this field, viz., Community Cloud and Mobile Cloud.

A.1 Public Cloud

Public cloud applications, storage, and other resources are made available to the general public by a service provider, using a free to all services or a pay per use model (Figure 2).

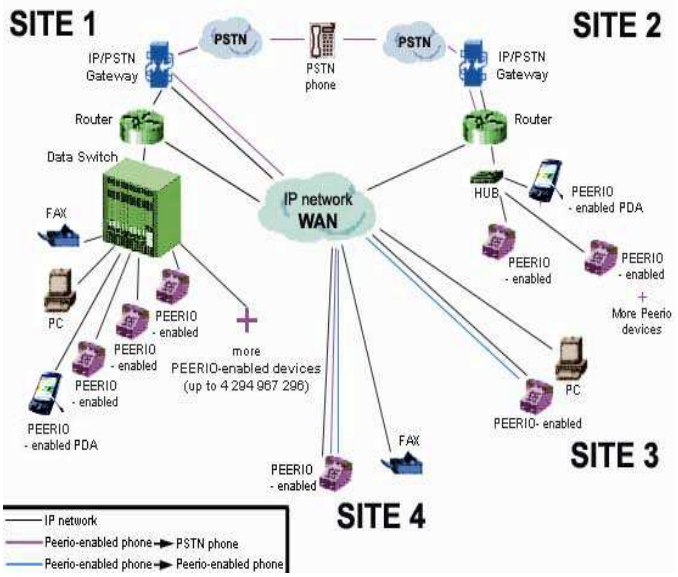

Fig. 2 Public Cloud

A.2 Private Cloud

Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally .It is also known as Internal

Cloud or Corporate Cloud. Marketing media that uses the words "private cloud" is designed to appeal to an organization that needs or wants more control over their data than they can get by using a third-party hosted service. In Figure 3, a diagram for private cloud has been shown. Using Virtual Middleware (VM) or Virtual data center, the company can run their private cloud services. Microsoft Azure, IBM, Sales force etc they run private cloud services.

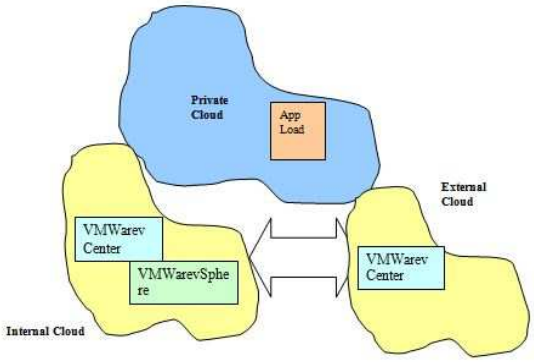

Fig. 3 Private Cloud

A.3 Hybrid cloud

Organizations may host critical applications on private clouds and applications with comparatively less security concerns on the public cloud. In case of hybrid cloud computing, both private and public type of cloud computing is combined together. This is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models.

By utilizing "hybrid cloud" architecture, shown in Figure 4, companies and individuals are able to obtain degrees of fault tolerance combined with locally immediate usability without dependency on internet connectivity. Hybrid cloud architecture requires both on-premises resources and off-site server-based cloud infrastructure.

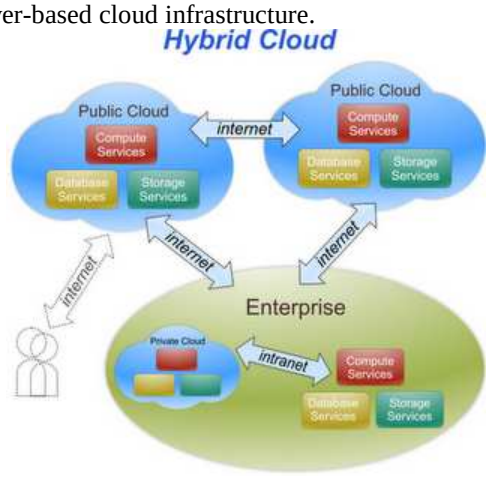

Fig. 4 Hybrid Cloud

A.4 Community Cloud

A community cloud in computing is a collaborative effort in which infrastructure is shared between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally. The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the cost savings potential of cloud computing are realized. Community cloud is a special type of service where a group of service providers united together and form a community depending on service type.

A.5 Mobile Cloud

Mobile cloud computing is the usage of cloud computing in combination with mobile devices. Cloud computing exists when tasks and data are kept on the Internet rather than on individual devices, providing on-demand access. In case of mobile cloud, Applications are run on a remote server and then sent to the user. Because of the advanced improvement in mobile browsers thanks to Apple and Google over the past couple of years, nearly every mobile should have a suitable browser. This means developers will have a much wider market and they can bypass the restrictions created by mobile operating systems. Mobile applications are a rapidly developing segment of the global mobile market.

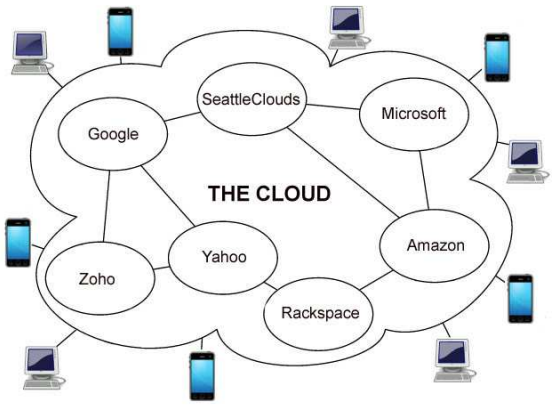

Fig 5 Mobile Cloud

Cloud Delivery Models

Cloud computing service providers deploy there services categorized mainly into these three following models:

- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Software as a service (SaaS)

A.1 Infrastructure as a service (IAAS)

It is the delivery of computer infrastructure (typically a platform virtualization environment) as a

service. Rather than purchasing servers, software, data center space or network equipment, clients instead buy these resources as a fully outsourced service. In this most basic cloud service model, cloud providers offer computers, as physical or more often as virtual machines, and other resources. The virtual machines are run as guests by a hyper visor, such as Xen or KVM. Examples of IaaS include: Amazon Cloud Formation (and underlying services such as Amazon EC2), Rackspace Cloud, Terremark and Google Compute Engine.

A.2 Platform as a service(PAAS)

Platform as a service or PaaS provides the Application Framework-as-a-service layer upon which software applications can be securely and reliably built. Industry Analyst firm Forrester describes PaaS as an externally hosted service that provides a complete platform to create, run, and operate applications. It is another SAAS, where this kind of cloud computing providing development environment as a service. In the PaaS model, cloud providers deliver a computing platform typically including operating system, programming language execution environment, database, and web server. Some examples of PAAS are Amazon Elastic Beanstalk, Cloud Foundry, Heroku, Force.com, EngineYard, Mendix, Google App Engine, Microsoft, Azure.

A.3 Software As a Service (SAAS)

This kind of cloud computing transfer programs to millions of users through browser. In the user's views, this can save some cost on servers and software. SAAS is commonly used in human resource management system and ERP (Enterprise Resource Planning). Google Apps and Zoho Office is also providing this kind of service.

B. Reasons for adapting Cloud Computing

The applications of cloud computing are practically limitless. With the right middleware, a cloud computing system could execute all the programs which a normal computer could manage to run. Potentially, everything from generic word processing software to customized computer programs designed for a specific company could work on a cloud computing system. Due to the following reasons cloud application are being adapted by the Industries and academics:

I. Clients would be able to access their applications and data from anywhere at any time. They could access the cloud computing system using any computer linked to the Internet. Data wouldn't be confined to a hard drive on one user's computer or even a corporation's internal network.

II. It could bring hardware costs down. Cloud computing systems would reduce the need for advanced hardware on the client side. You wouldn't need to buy the fastest computer with the most memory, because the cloud system would take care of those needs for you.

III. Corporations that rely on computers have to make sure they have the right software in place to achieve goals. Cloud computing systems give these organizations company-wide access to computer applications. The companies do not have to buy a set of software or software licenses for every employee.

IV. Servers and digital storage devices take up space. Some companies rent physical space to store servers and databases because they don't have it available on site. Cloud computing gives these companies the option of storing data on someone else's hardware, removing the need for physical space on the front end.

V. Corporations might save money on IT support. Streamlined hardware would, in theory, have fewer problems than a network of heterogeneous machines and operating systems. Due to such a great applicability, the popularity of cloud computing is continuing to soar in spite of being a newly developed technology in the very recent years.

C Characteristics of Cloud Computing

Some unique features of cloud computing has made this newly growing up technology a market leader for the recent era.

C.1 Automation is one of the biggest features of cloud computing. It gives businesses the peace of mind they need to focus on their core business. They no longer need to set up teams to take care of tasks such as back-ups and system updates.

C.2 Cost is claimed to be reduced and in a public cloud delivery model capital expenditure is converted to operational expenditure. This is purported to lower barriers to entry, as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing.

C.3 Recoveries are extremely fast with cloud computing. Thus, you don't lose any unnecessary time here. Cloud computing also allows businesses to go mobile. You no longer need to be location-dependent for work.

C.4 Virtualization technology allows servers and storage devices to be shared and utilization be

increased. Applications can be easily migrated from one physical server to another.

C.5 Multitenancy enables sharing of resources and costs across a large pool of users thus allowing for Centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.)

C.6 Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places

Attack Vectors in Cloud

Attack vectors, one of the common and popular term in the world of cloud security, is the route or path through which the attacker gets entered into the system, mainly due to nefarious purposes [7][8]. They take advantage of known weak spots to gain entry. Many attack vectors take advantage of the human element in the *system*, because that's often the weakest link. Emails, the attachments carried by an email or the deception may be treated as an attack vector for malicious purposes. Hoax as an attack vector can damage the network also. Even though they don't attack computers directly, ignorance and credulity is the attack vector here as it is being spread by multiple numbers of people. Web pages can be used as an attack vectors too. They can be rigged to do a number of things -- virtually anything that a malicious email attachment can do. They take advantage of the power that modern browsers have to access several program languages -- Java, Javascript, ActiveX and Microsoft Word macros. Several Attack vectors have been discussed in the following few paragraphs followed by the threats or attacks over the cloud system.

i) Denial of Service (DoS) attacks

This is a very common attack vector launched by an eavesdropper when hackers overflow a network server or web server with frequent request of services to damage the network, server could not legitimate clients' regular requests of the services. In cloud computing, hackers attack on the server by sending thousands of requests to the server that server is unable to respond to the regular clients in this way server will not work properly [9].

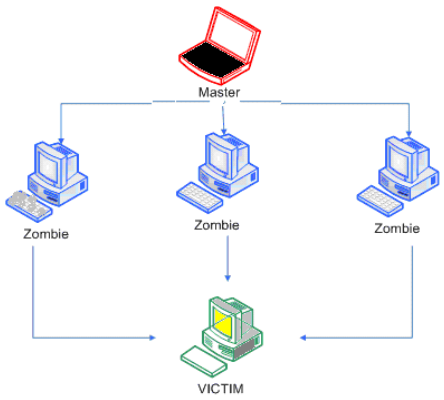

Fig. 6 DOS Attack

In the Figure 6, we have shown an image for the Denial of service attack where the master launches an attack through compromised zombie network.

ii)Cloud Malware Injection Attack

Usually when a customer opens an account in the cloud, the provider creates an image of the customer's VM in the image repository system of the cloud. In case of a malware-injection attack, the attacker takes an adversary attempts to inject malicious service or code, which appears as one of the valid instance services running in the cloud. If the attacker is successful, then the cloud service will suffer from eavesdropping. The main idea of the Cloud Malware Injection attack is that an attacker uploads a manipulated copy of a victim's service instance so that some service requests to the victim service are processed within that malicious instance. In order to achieve this, the attacker has to gain control over the victim's data in the cloud system (e.g. using one of the attacks described above). This attack is the major representative of exploiting the service-to-cloud attack surface.

iii) Distributed Denial of Service Attack (DDOS Attack)

Distributed Denial of Service is a special type of DOS attack where multiple compromised systems are used, which are usually infected with a Trojan and used to target a single system causing a Denial of Service (DoS) attack. Victims of a DDoS attack, shown in Figure 7, consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack. This attack is now a days becoming a popular attack for cloud services [10].

In this attack, the eavesdropper being the master component launches the attack on the victim, using a compromised network which is in turn divided into two separate layers. This attack is very vulnerable especially for shared environment like cloud, where sometimes even the service provider

does not know from where the service has come to them and where the data has been stored.

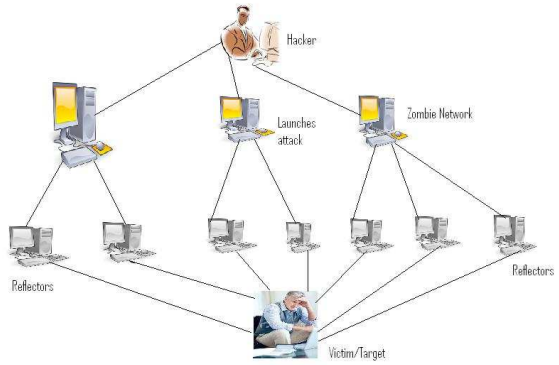

Fig. 7 Distributed DOS Attack

iv) Side Channel Attack

Within a piece of hardware that has multiple virtual machine resources are shared which can be used as a way to side channel data from one virtual machine to another. This type of attack is based on the shared resources between virtual machines within the same hardware. An attacker being successful in neighboring a target can then use various methods for intercepting data being sent and received from the other virtual machine. This form of security risk has been documented and there are many methods for preventing this type of attack.

v) Cross Site scripting Attack

Cross-site scripting attack (XSS) is a security exploit in which the attacker inserts malicious codes into a link that appears to be from a trustworthy source. When someone clicks on the link, the embedded programming is submitted as part of the client's Web request and can execute on the user's computer, typically allowing the attacker to steal information. So, instead of going to the original server address it will be directed to the malicious site. This attack has a great impact on cloud computing. SQL injection attack is a special type of such attack [10][11].

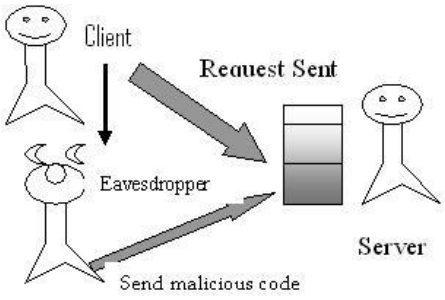

Fig. 8 Cross Site scripting attack

vi) Man-in-the Middle attack

Man in the middle attack, shown in Figure 9, also known as fire brigade attack is carried out when an attacker places himself between two users. Anytime attackers can place themselves in the communication's path, there is the possibility that they can intercept and modify communications, tamper data [12].

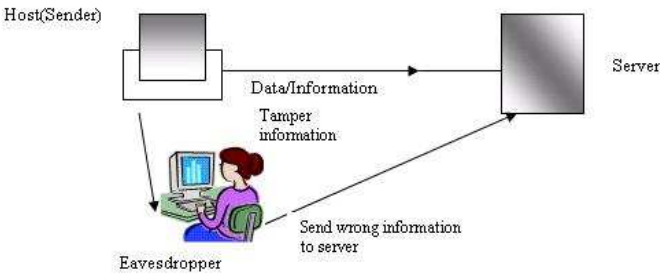

Fig. 9 Man in the middle attack

vii) Wrapping attack

XML signature Element Wrapping is the fine renowned attack for web service [13]. This attack is done by duplication of the user account and password in the log-in phase so that the SOAP (Simple Object Access Protocol) messages that are exchanged during the setup phase between the Web browser and server are affected by the attackers. Attacker targets the component by operating the SOAP messages and putting anything that attacker likes, as shown in Figure 10.

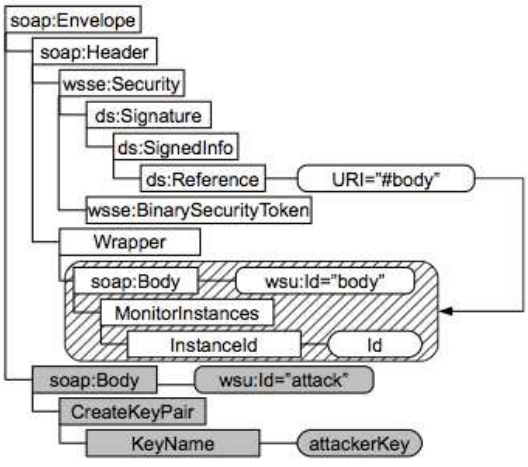

Fig. 10 Wrapping Attack

viii) Flooding attack

In this attack, the attacker launches the attack openly. The most significant feature of cloud system is to make available of vigorously scalable resources. Cloud system repeatedly increase its size

when there is further requests from clients, cloud system initialize new service request in order to maintain client requirements. Flooding attack is basically distributing a great amount of meaningless requests to a certain services which flood the server [11] [14].

Once the attacker throw a great amount of requests, by providing more recourses cloud system will attempt to work against the requests, ultimately system consume all recourses and not capable to supply service to normal requests from user. Then attacker attacks the service server. DOS attacks cost extra fees to the consumer for usage of recourses. In an unexpected situation the owner of the service has to compensate additional money. Counter measure for this attack is it's not easy to stop Dos Attacks.

ix) Network Sniffing Attack

Network sniffing attack is more critical issue of network security in which un-encrypted data are hacked through network for example an attacker can hack passwords that are not properly encrypted during communication. If the communication parties not used encryption techniques for data security then attacker can capture the data during transmission as a third party. Counter measure for this attack is parties should used encryption methods for securing there data [13][15].

x) Problem of Cheap data and data analysis

Access of data in cloud is cheap. But along with this it brings some problems. Because of the cloud, attackers potentially have massive, centralized databases available for analysis and also the raw computing power to mine these databases. Synchronizing data is a problem. An example of indirect data-mining that might be performed by a cloud provider is to note transactional and relationship information. But this problem can be solved by proper tracking of IP

xi) Port Scanning

There are some issues faced by the cloud providers regarding port scanning that could be used by an attacker as Port 80(HTTP) is always open that is used for providing the web services to the user. Other ports such as 21(FTP) etc are not opened all the time it will open when needed therefore ports should be secured by encrypted until and unless the server software is configured properly [16]. The approaches has been taken to dissolve this attack is that firewall is used to secure the data from port attacks.

xii) Accountability Check problem

The payment method of cloud system is "No use No bill". When a customer launches an instance, the duration of the instance, the amount of data transfer in the network and the number of CPU cycles per user are all recorded. Based on this recorded information, the customer is charged. But with the accountability check problem, an attacker has engaged the cloud with a malicious service or runs malicious codes, consuming a lot of computational power and storage from the cloud server and as a result, the legitimate account holder is charged for this kind of computation which he or she have not taken in actual. Hence, a dispute arises and business reputations are hampered.

Conclusion

Cloud computing offers real benefits to the organizations seeking opportunity to the competitive edge in economy. The attractive price, well build infrastructure and ability to pay for 'as needed' services will drive more businesses to move towards cloud computing adaptation. But, as always, the revolution comes with some problems, security issues in cloud computing is always a major concern for the cloud system. In this paper, we have discussed about some issues and several well known attacks related to those issues that may hamper the cloud services directly or indirectly. The privacy and security area in cloud computing leaves an ample scope for the cloud researchers and developers towards the design and development of proper measurement tools to quantitatively measure the impact of different types of attack vectors so that justified evaluation of threats could be done and proactively appropriate countermeasures could be taken. It is observed that all threats are not of same value, i.e., not equally harmful. Where, some are critically dangerous, some could be ignored even, and thus the requirement of identification, categorization and proper measurement of the harmfulness of different types of threats or attack vectors have become essential primarily for the cloud providers using proper metrics and tools to increase the province of their business by spreading the domain of the concerned technology.

References

[1] P. Mell and T. Grance, "Draft NIST working definition of cloud computing - v15," *21. Aug 2009*, *2009*.

[2] Resse, Mather, "Cloud Application Architecture: Building Applications and Infrastructure in the Cloud", SPD O'Reilly publication, 2009

[3] http://en.wikipedia.org/wiki/Cloud_computing.

[4] Stevenson, "Cloud Security and Privacy", SPD O'Reilly publication, 2010

[5] Mohit Mathur, KLSI, "Cloud computing Black Book", Wiley Publication, 2012

[6] Wilder, “Cloud Architecture Patterns”, SPD O’Reilly publication, 2012
[7] Ajey Singh, Dr. Maneesh Shrivastava “Overview of Attacks on Cloud Computing” published on International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012.
[8] http://searchsecurity.techtarget.com/definition/attack-vector.
[9] B.Meena- Dept. of Information Technology, ANITS, Visakhapatnam, AP, Krishnaveer Abhishek Challa , Dept. of Electrical Engineering, Blekinge Institute of Technology, Sweden, ” Cloud Computing Security Issues with Possible Solutions”, IJCST Vol. 3, Issue 1, Jan. - March 2012.
[10] Kazi Zunnurhain and Susan V. Vrbsky, Department of Computer Science, The University of Alabama, “Security Attacks and Solutions in Clouds”.
[11] Mario Heiderich, Marcus Niemietz, Felix Schuster, Thorsten Holz, Jörg Schwenk, “Scriptless Attacks –Stealing the Pie Without Touching the Sill”
[12] Sara Qaisar, Kausar Fiaz Khawaja (Corresponding Author), “Cloud Computing: Network/Security Threats And Countermeasures” published on Interdisciplinary Journal Of Contemporary Research In Business on January 2012, VOL 3, NO 9.
[13] Timotthy K. Buennemeyer, “A Strategic Approach to Network Defense: Framing the Cloud”, Autumn 2011
[14] Muhammad Imran Tariq, Department of Computer Science and Information Technology, University of Lahore, “Towards Information Security”
[15] Nelson Gonzalez, Charles Miers, Fernando Red Igolo, Marcos Simplıcio, Tereza Carvalho, Mats N¨aslund and Makan Pourzandi, “A quantitative analysis of current security concerns and solutions for cloud computing”, Journal of Cloud Computing, Springer Open Journal,2012 “Security guidance for critical areas of focus in cloud computing v3.0”, Cloud Security Alliances, 2