Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 11, November 2014, pg.577 – 586

RESEARCH ARTICLE

A Study of Security Structure System in Cloud Computing

Dr. P.K.Rai[1], Rajesh Kumar Bunkar[2]

[1]Computer Centre, APS University, Rewa, M.P., India

[2]Research Scholar, MGCGV Chitrakoot, Satna, M.P., India

[1] pkrapsu@gmail.com; [2] bunkar.rajesh@gmail.com

Abstract— Security is the major obstacles of the long dreamed vision of cloud computing. The sensitive application data are moved into the cloud data centres and run on virtual computing resources in the form of virtual device. The user concerns about cloud computing is its security. Enterprise data centres, Internet Data Centres (IDC) and service provider's offer racks and networks, and the remaining devices have to be prepared by users with servers, firewalls, and storage devices etc. Under cloud computing, the backend resources and management architecture of the service is top privacy for user. In cloud computing atmosphere security investigation and evaluation of privacy, security and trust issues by a quantifiable approach are the prime concern of security. In this paper we have discussed physical and logical security of cloud computing.

Keywords— Authentication, Data Security, Encryption, Physical security, Logical security, security precautions, OpenID

I. INTRODUCTION

Cloud Computing is defined by a large-scale distributed computing paradigm that is driven by financial system of level, in which a collection of distracted, virtualized, scalable, managed compute rule, stockroom space, platform, and services are deliver on order to external customers over the internet [7]. Security may be defined as preservation of privacy, integrity and availability of information, and other properties such as accuracy, responsibility, non-repudiation and reliability can also be implicated [2]. The term security is a conceptual term that can be thought as an entity that aims to provide protection to anything that is risk. Security is separated into two categories: physical and logical security [1]. Physical security explain all feasible security methods that one might take in order to protect their corporate infrastructure and equipment (buildings, computer rooms etc). Logical security would describe any security measures that one might take and that are not involved in physical security (firewalls, intrusion detection and prevention, authentication, encryption and VPNs etc).

II. PHYSICAL SECURITY

Physical security [1] can be defined as all the necessary measures (Structure System and implementations) that a cloud customer or cloud vendor might take in order to protect their infrastructure/facilities. Physical security contains a set of policies and procedures but it cannot be defined in a certain way. Every individual or company might implement different physical security measures. Security is an abstract term and can be in more than one form. To be more precise, there will be an analysis on the physical models that Microsoft, Google and Cisco implement to their facilities in order to protect. Microsoft has adopted a certain strategic plan for the management of accessing their physical resources. They have also created a particular business model which aims to ensure balance between what Microsoft considers important in their physical security scheme (technology, monitoring and response along with the corresponding administration of those three factors). This model is called the Weighted Business model (WBM) and is being depicted in the following figure:

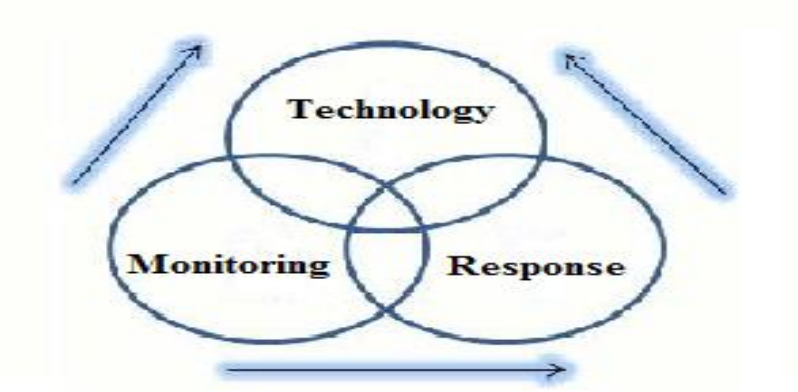

Fig.1 Microsoft's Weighted Business Model [1].

Microsoft focuses into the following key physical security elements-

a. Deterrence value.
b. Remote monitoring.
c. Precision response.
d. Off-the-shelf infrastructure.
e. Utilize Microsoft and partner products.
f. Remotely managed IP devices.
g. Defense in depth.

Forensics/investigative model.

I. Reliability.
II. Sustainability.

All security key elements lead Microsoft in some very important business benefits:

1) Reduced costs.
2) Improved security.
3) Scalability and Extensibility.
4) Business continuity.

There is a variation on the physical security schemes that are being used based on the location and regional risks. Despite the differences in physical security schemes between different locations and regions, Google implements a set of standard physical security controls to all of their buildings and facilities. Those controls are:

1. Alarm systems.
2. Electronic card access control systems (custom designed systems).

3.Cameras to secure either the interior or the exterior perimeter of the facilities.
4.Security guards.

Physical security is the most important priority for a cloud vendor because without the necessary measures and technological background cloud customers would not be able to trust their data and services in the cloud. Except all the methods and equipment, physical security in general should be formed from some or all of the below security measures:

1.Security personnel.
2.Surveillance monitors and tape devices.
3.Limit access to critical areas where networking equipments and data are held.
4.Use fire detection and prevention mechanisms.
5.Use security alarms that interact live with the nearest police department and
6.Security alert personnel in real time.
7.Use key cards for accessing data rooms or different departments and sections within the infrastructure.

III. LOGICAL SECURITY

Logical security [1] contains all the necessary measures and configurations that cloud vendors should implement in order to protect their networking infrastructure and services (routers, switches, demilitarized zones, virtual private networks etc.). Physical security ensures that equipment is held in a safe environment while logical security provides security within the networking environment. The first security Mechanism that is going to be examined is authentication. There will be an effort to cover all possible authentication schemes and evaluate their effectiveness in a cloud computing environment.

Authentication: is considered to be the most important process for a cloud customer because through authentication one can access their personal data and services. Authentication is also important for the cloud vendors because they are able to assign certain roles and responsibilities to their employees and provide access only to sections within their job roles. There are many different authentication schemes that each cloud vendor implements depending on how safe and trustworthy they need to make their service or application. For instance, there is simple authentication which is a process where a user is required to enter a username and a password, single sign-on, where a user is able with just one account to access different sites and services, one time passwords, where a user is forced to use a random password each time they try to log in to a service or application, two-factor authentication and public key cryptography.

Simple authentication: This form of authentication is the simplest and the more insecure among authentication schemes. A cloud customer is only required to enter a username and a password in order to gain access to the desired services or applications. The Fig.2 shows Microsoft's Hotmail sign-in form.

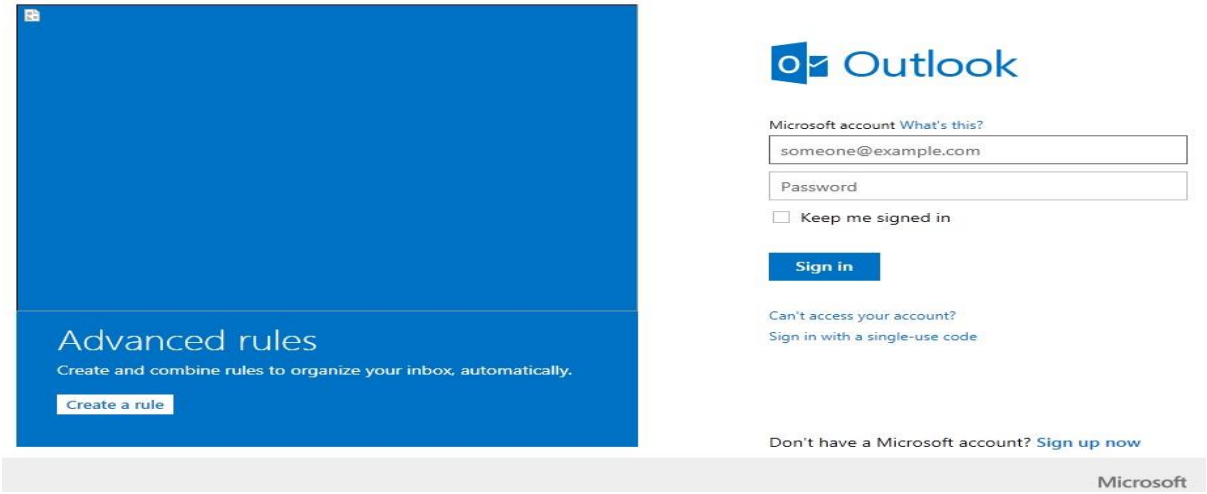

Fig.2 Hotmail sign-in form [4]

Authentication is considered to be the more insecure authentication process; however, it is not that insecure. The interaction between cloud customers and the services/applications is being made through the HTTPS protocol (Hypertext Transfer Protocol Secure) instead of HTTP. All cloud providers that offer services and applications with simple authentication they give as an option the registration of a secondary e-mail address in case where an account has been hijacked.

Single sign-on: Single sign-on is a method through which a user is able to gain access on multiple related but independent software systems. Users enter their passwords only once and they are able to access any desired service or application without the need of re-entering their credentials.

Single Sign on Benefits: Ability to enforce uniform enterprise authentication and/or authorization policies across the enterprise end to end user audit sessions to improve security reporting and auditing, removes application developers from having to understand and implement identity security in their applications [5].

There is also an open standard that is used to handle single sign-on processes called OpenID. OpenID is being implemented by many cloud vendors like Google, Yahoo, and IBM etc. When a user creates an OpenID account then enters the credentials of all supported services within the OpenID interface. This process is being made only once. Afterwards, all related services and applications are accessible though the OpenID account. The Fig. 3 depicts the processes that are being made during authentication with OpenID protocol.

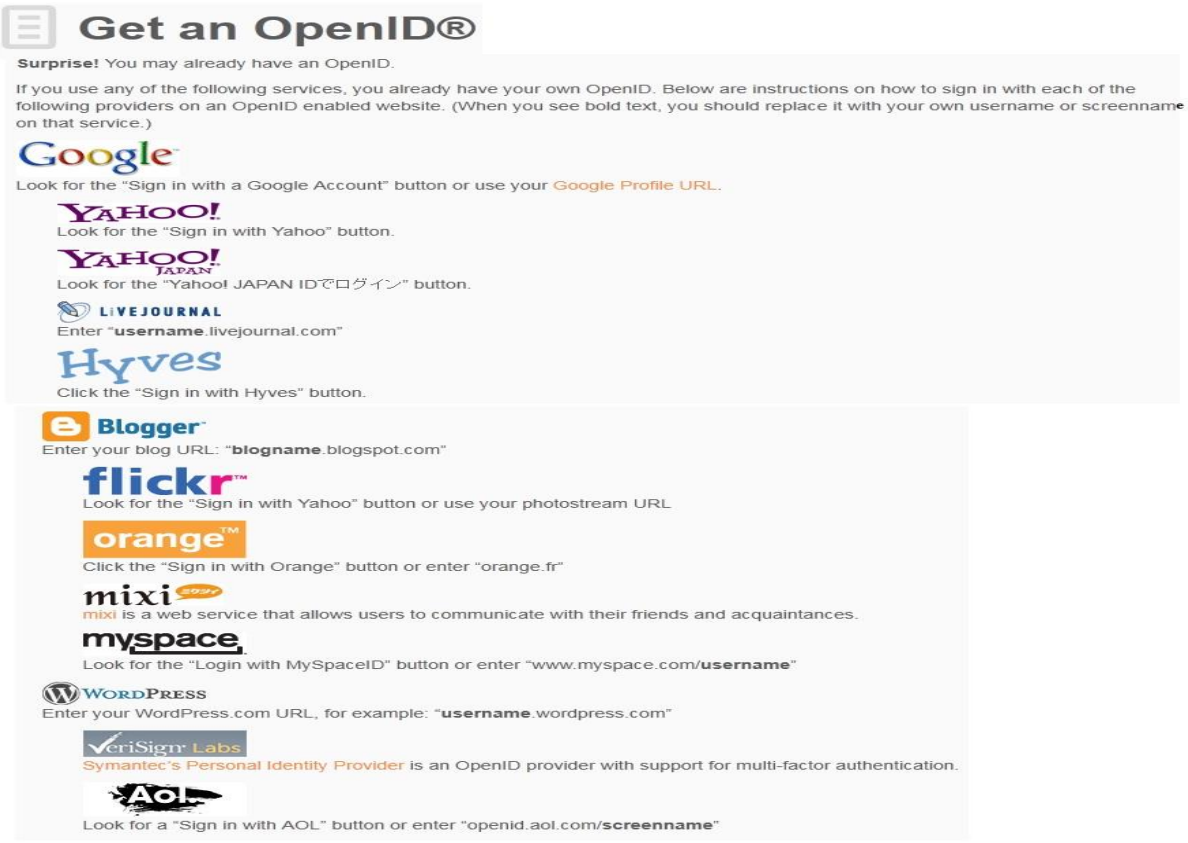

Fig.3 OpenID [6].

One-time passwords: are used in order to increase security during sign-on process. Conventional passwords that are used in a sign-on process typically have a policy to change occasionally or never and for that reason there are more possibilities to be compromise. One time passwords can be also time coordinated or counter synchronized passwords. In both cases cloud customers need to keep to their possession a small electronic device that handles one-time passwords. Each cloud vendor might either implement time or counter synchronized passwords, time synchronized passwords contain a critical risk. If time synchronization between the electronic device and the server fails then users would not be able to authenticate themselves. On the other hand, counter synchronized passwords synchronize a password counter between the electronic device and the server. To get a better understanding on how one-time passwords operate. Fig. 4 shows a typical one-time password scheme.

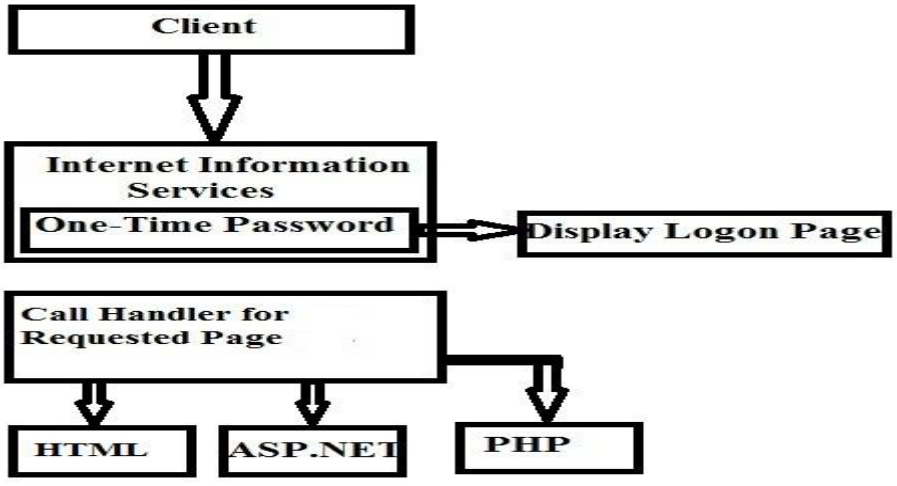

Fig.4 **One time password scheme[1]**

Two factor authentication [1]: is a method that requires at least two authentication processes. This method is probably the most secure among authentication processes because even if a user becomes a victim of a hacking activity and their credentials gets compromised, the hacker would not be able to access to the services and applications that are attached to that account because there would be required a second authentication factor. In most cases the second authentication factor is a short message service (SMS) or a call from the provider that reveals to the cloud customer the second factor authentication password. A representative example of a two factor authentication process is Google's two factor step verification mechanism. Google requests from their customers to register their phone numbers and choose between receiving a text message or a phone call in order to get the second authentication factor password. There is also a third option to users that own smart phones to download and install Google authenticator application and generate by themselves the second factor authentication password.

Encryption: As it is already known, cloud computing is based on the public internet and though suffers from many security risks and vulnerabilities. Cloud vendors use encryption [1] techniques in order to encode exchanging messages between cloud customers and/or cloud vendors. Encryption is a technique used to prevent eavesdroppers and hackers from reading the information that is being sent or exchanged between two entities. In contrast to authentication, encryption is not only cloud vendors' responsibility but cloud customers are also responsible for encrypting their data and information before sending them to the cloud. The most common encryption scheme is composed by the use of Hypertext Transfer Protocol Secure (HTTPS) and Secure Sockets Layer (SSL). SSL provides a secure communication channel between the cloud customer and the cloud vendor's web server. Data travel through that communication channel encrypted over the public internet. The communication path is being created only when the client verifies that the SSL certificate of the server is trustworthy, a process called SSL handshake. Common SSL handshake process is shown in the Fig. 5:

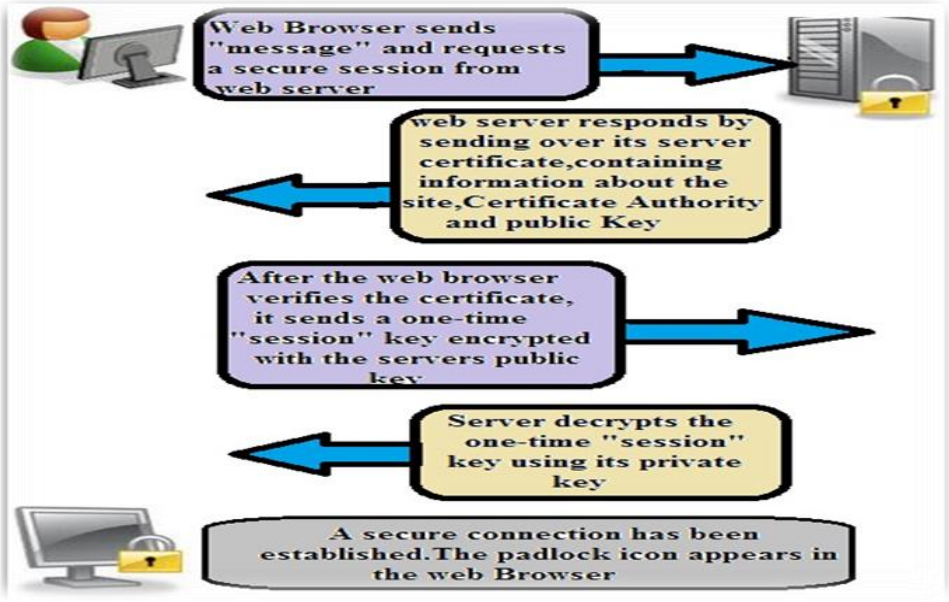

Fig.5 SSL handshake [1].

Encryption can be either symmetric or asymmetric. Symmetric encryption is the one that uses the same key for encryption and decryption while asymmetric encryption uses deferent keys for encryption and decryption processes. Fig.6 shows a symmetric encryption scheme and Fig.7 shows an asymmetric encryption scheme.

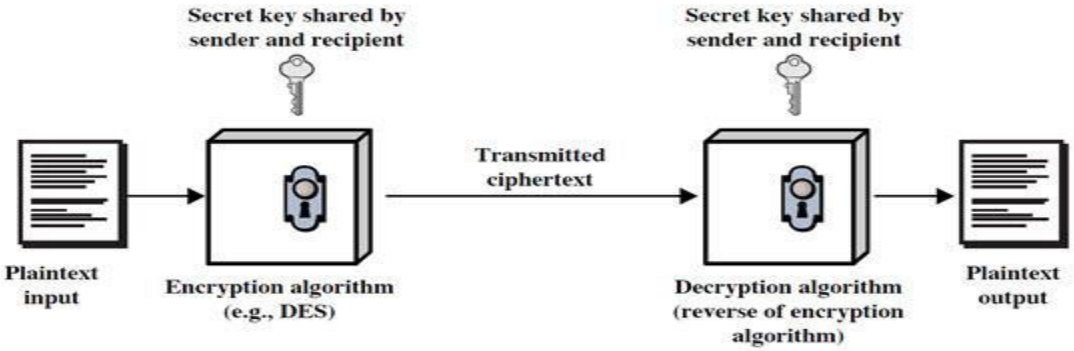

Fig.6 Symmetric Encryption scheme [1].

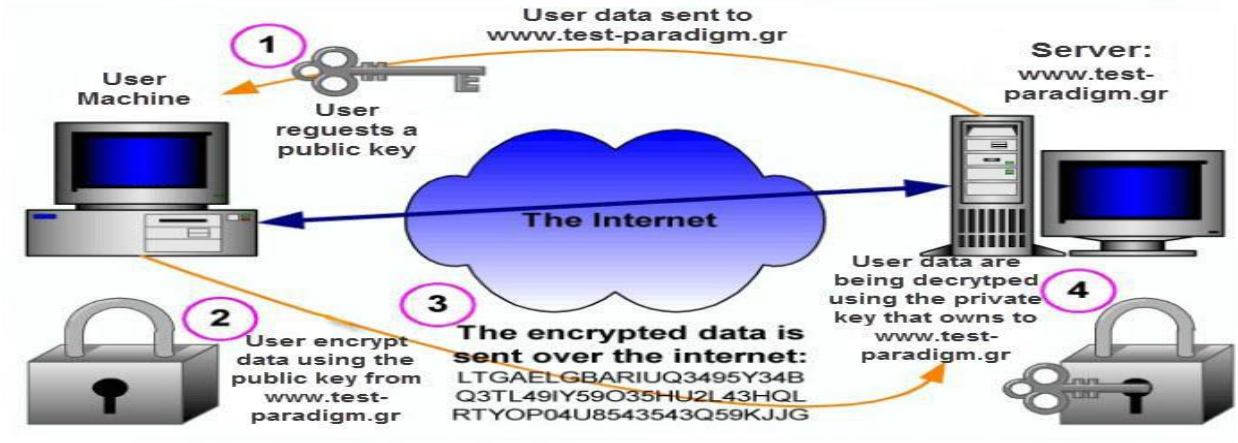

Fig.7 asymmetric encryption scheme [1].

Data Security: Data security technique is built on three basic principles confidentiality, integrity and availability. Confidentiality refers to the supposed hidden the actual data or information, especially in the military and other perceptive areas, the confidentiality of data are the more stringent requirements. Since, in cloud computing, the data are stored in data centre, the security and confidentiality of user data is even more important. The supposed integrity of data in any state is not subject to the need to guarantee unauthorized erasure, modification or damage. The availability of data means that users can have the expectations of the use of data by the use of capacity [3].

Firewalls : In a cloud computing environment firewalls [1] form the first line of defence against many different types of attacks like Denial of service (DoS) attacks, TCP flooding, malware, viruses, worms, etc. Firewalls are responsible to handle traffic from and to the internal network and allow only requests that are permitted. Permissions to incoming and outgoing traffic are being held in IP tables. Firewalls are able to perform many different and extremely important roles like packet filtering, network address translation (NAT), to act as proxy services, provide encrypted authentication, form virtual private networks (VPNs), and perform virus scanning and content Filtering. A typical firewall scheme between cloud customers and cloud vendors is being depicted in the Fig. 8.

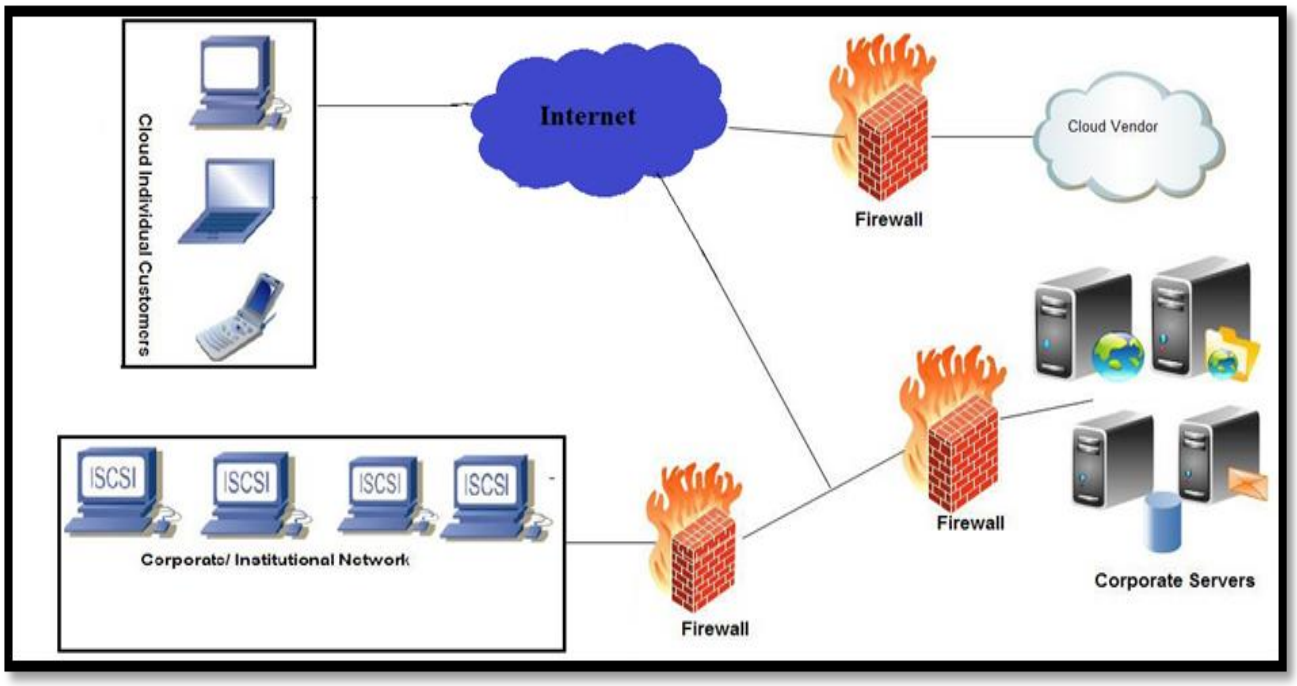

Fig. 8 Firewall scheme [1]

Cloud firewalls perform the same actions that a corporate firewall would perform and protect cloud customers from unauthorized users and fake requests. For instance if a cloud vendor provides e-mail services then it only allows traffic to port 25 for the users that have managed to authenticate to their service. If additionally the cloud vendor offered ftp services then the only ports that would be opened are port 25 and port 21 and so on. Firewalls operate by consulting the IP tables that exist within their structure and allow only registered entries to access or leave the cloud infrastructure.

Intrusion Detection Systems (IDS): In addition to firewalls, cloud vendors also implement intrusion detection systems. Like firewalls intrusion detection systems can either be hardware devices or software applications. A cloud vendor that implements IDS offers to their clients monitoring to network or system activities regarding malicious activities or even strategy violation. All this monitoring is being produced in reports to a management station. IDS are being implemented to target possible incidents and log information about them. Furthermore, the reporting services can be used in order to examine possible threats and provide the appropriate security fixes in order to increase security. IDS systems can be found in three different forms:

1) Network intrusion detection systems (NIDS) are the system monitoring network traffic and multiple hosts in order to identify possible threats.
2) Host-based IDS (HIDS) consists of a host that contains an agent that analyses systems calls, activities and states of hosts and app logs in order to identify intrusions. There are also software agents to every client machine containing sensors that capture network traffic and perform content analysis in order to find malicious traffic.
3) Stack-based IDS, such IDS systems can be thought of as the growth of HIDS. This is used to analyse and observe packets while they move through the TCP/IP stack.

Identity and Access Management (IAM): are targeted for lifecycle and compliance identities, accounts and the corresponding entitlements. The features that IAM offers to cloud customers are being outlined below:

1) Strong authentication.
2) SSO (Single Sign-On).

3) Amalgamation with Software-as-a-Service providers and private parties.
4) Identity lifecycle automation.
5) User self-service.
6) Administration and access control are centralized.
7) Transaction auditing.
8) User provisioning and identity awareness.
9) Identity intelligence and transparency.

Other security precautions: Cloud vendors implement the following security measures in order to increase security to their infrastructures:

1. Equipment: The equipment that a cloud vendor uses has more than one power supplies in order to perform failover in case of a power supply breakdown. Routers, switches and servers have at least two power supplies which makes them available all the time. Furthermore, there is no need for downtime during the repair process of the broken parts because it can be done while the machine is online. There are a few cases where the equipment should be switched off in order to perform system maintenance.
2. Power supply vendors: Most cloud vendors have more than one power supply vendors where it is possible. Vendors with two power supply vendors can assure their customers that there will not be a downtime where power failure might occur. Even cloud vendors with one power supplies have pre-installed uninterruptible power supply units, also known as UPS, in order to maintain their services up for a few hours more when there is an issue with the power supply.
3. Internet providers: All cloud vendors cooperate with at least two cloud vendors. One acts as a backup solution in case of service failure of the primary internet vendor.
4. Data backup: Data are being stored to more than one hard disk drive and in different locations. As a result, even if the whole infrastructure of a particular area collapses, cloud customers would be able to access their data. Backup operation occurs to virtual hard disk drives and when there is a system crash that cannot be fixed, cloud vendors restore the damage from the backed up VHD files.
5. Disaster recovery plan: In data backup, all cloud vendors' performs a disaster recovery plan. There are mirror images of all machines and equipment in another geographical area so that in case where the infrastructure at one place is burned or an earthquake destroys the facilities, cloud customers would be served from the other location as well. In order to achieve such a difficult project cloud vendors perform real time synchronization between the two areas. Disaster recovery plan is really important procedure and should be taken into consideration from users and companies that are likely to move their data or services to the cloud.

IV. CONCLUSIONS

The present study is important to perform an evaluation on security structure system and their effectiveness in cloud services and applications. It is also important to describe upcoming trends and security structure system that might exist in the near future and increase security to make the cloud computing environment more attractive in terms of safety for the cloud consumers. First is physical security, as it is the first level of security. We conclude that current security measures are more than adequate and can provide security to the maximum satisfying even the more demanding cloud customer. The second part of security is logical security. There are many cloud applications and services that use simple authentication and the user is exposed in case of a hacking activity. There should be a short of arrangement between all cloud vendors in order to come to an agreement regarding the minimum requirements for a strong and secure authentication scheme. The most important factor is

encryption. It should be with the encryption and decryption keys. Firewalls have been the first line of defense in many networks for ages and while there were changes regarding their hardware gear and their performance, configuration still remains the same. Intrusion detection systems wherever are used are able to provide deep and real-time protection. Identity and access management systems also provide a centralized and complete security solution.

References

[1]. Katis Dimitrios, "Security Mechanisms in Cloud Computing", Jan. 2013.
[2].ISO (2005) 27001: Information Security Management – Specification with Guidance for Use.
[3].Dai Yuefa et.al, "Data Security Model for Cloud Computing", Proceedings of the 2009 International Workshop on Information Security and Application (IWISA 2009), ISBN 978-952-5726-06-0, Qingdao, China, November 21-22, 2009.
[4]. https://mail.live.com/in.
[5]. http://www.authenticationworld.com/Single-Sign-On-Authentication.
[6].http://openid.net/get-an-openid/
[7].Ian Foster, Yong Zhao, Ioan Raicu, Shiyong Lu. "Cloud Computing and Grid Computing 360-Degree Compared", Grid Computing Environments Workshop, 2008, GCE'08, 12-16 Nov.2008.

