IMPLEMENTING USER AUTHENTICATION SERVICE FOR CLOUD NETWORK

[1]Masood Shah, [2]Ahmed khan
[1]Department of Computer Science SZABIST, ISB, Pakistan
[2] Department of Information Security, NUST, Pakistan.
[2] Department of Computer Science, COMSATS, Pakistan.
[1] engg.cisco@gmail.com, [2] ahmed.khan@comsats.edu.pk

ABSTRACT*- The use of the cloud is completely based on the internet. The improvement in internet speed and bandwidth all over the world has made cloud computing more popular. Enterprise companies are migrating or planning to shift their infrastructure on cloud. Companies migrated on cloud, adopt different authentication schemes in addition to provide actual services on the cloud. User authentication is additional overhead that they have to look after in addition. Our research is based on the idea to provide central authentication technique to different companies that require authentication to provide access to their users instead of adopting some user authentication techniques by them. We have not only proposed the model but implement it as well as a prototype.*

INTRODUCTION

The cloud computing is a concept in which there are two parties. The one party is that which give services to the other party and that party is called service provider. The service provider takes money from those people, who use these services. The other party is that which uses these services and that party is called user or consumer or client. The user gives money to the service provider on the use of services offered by them. All these services are virtual not real. These services are used through the internet. If a user wants to use the services of the cloud then they have to register on the cloud. The cloud gives him a password and user name. Then the user can connect to the cloud through the internet give his password and user name. Then can use the services of the cloud. The money that the user gives to the cloud is just like the electricity bill. The money that the user gives to the service provider is based on how much space they required, what type of speed and what type of security they required etc.

There are three types of client. One is the mobile user which use the services of the cloud through the mobile such is I-phone, Smartphone, blackberry etc., the second is a thin client, which have no hard disk. All the work is done on the cloud server. And only the result is displayed on the thin client. That result is also stored on the cloud server. The third type is the thick client which has a hard disk. The cloud server store information, but thick client also stores some information.

The benefit of the thin client is that no one can thief it. But the drawback is that every information is stored in the server. So a large space is required.There are many companies which offer the services of the cloud computing. The first one is the Amazon, which has offered the elastic cloud computing and simple storage services in 2006. The Google has also offered has cloud services. The services provided by IBM is blue cloud. Which have a platform and data storage centers. Microsoft has also offered window azure in 2008. The b platform of the azure is the belt on the internet. So the cloud goes from the pc to the internet. There are three types of cloud computing. One is public cloud. In this the services are public which are accessed through the public network from everywhere. The second type is the private cloud. In which the private services are accessed through the private network. The third is hybrid cloud. This is the combination of the public and private cloud. In the hybrid cloud some services are private and some are public. The services provided by the cloud are categorized as the SPI. The SPI provides the following services. The first layer in the SPI model is the **SaaS**. In this the user has given software to use. This is usually used in the thin client. The second layer of the SPI model is the **PaaS**. In this, the service provider gives platform to the user to develop software for himself.

The service providers provide everything that a developer need. The final layer of SPI model is the infrastructure as a service **IaaS**. In which the user has to manage the resources such is storage, database, server etc .The general architecture of the cloud is described as one is the authentication server. Which authenticats the user. The other is the user. Which use the services. Third is servers which provide services to user. First the user authenticates himself to the authentication server. After successful authentication user get permission to use the services.

With the large bandwidth and high speed of the internet the use of the cloud is increased. Because the cloud is accessed through the internet. The people save their cost of storage, maintenance and security etc. by the use of cloud services and pay to them. 80% of the enterprises use the cloud services in 2010. It is possible that in 2012 approximately 1000 people will use the cloud services. The problems which are to the internet are also in the cloud. Because the cloud is based on internet the first problem is the security.

LITERATURE REVIEW

In [2] Stolfo *et al* discuss about that how we store our personal and business data and how we protect in a cloud environment. The security of data in cloud environment is vulnerable up to some extent. Even cryptography did not provide full security to the data. There are new challenges for security in cloud in the present time, but the new technology use in cloud computing is decoy technology. It supervises and sense unusual data access. Suppose when an illegal access is detected and confirm so the system produce large amount of decoy data for attacker to cut off his access to the real user data. The example is practiced for data security in cloud computing. Every Business that may be small or medium size, all of them are taking so much interest in cloud computing. Because cloud computing gives them a data protection and a huge amount of memory usage remotely or virtually. The Example given in this paper is of data theft it is the most serious attack in cloud computing. The top threat to cloud computing by cloud security Alliance is when the attacker is malicious insider and majority of user know this threat.

In this paper [3] Yang *et al* describes about DDoS attacks and describes the mechanism that how to recover or trace

back the attack. Cloud computing is having so many characteristics like centralized security of every data and process, high availability, but still there are so many security challenges for cloud computing like DDoS attacks which can give a heavy loss to an organization in the form of degradation. This is a key point for cloud computing that how to deal with these challenges. Basically DDoS is attack on availability of services because cloud computing is based on recourse sharing at different levels like network level, application level, host level so DDoS is a big threat for these resources.

In this paper, we study different approaches like trace back Approach, which is Service Oriented Architecture for the identification of exact information about the attack on cloud, is another approach detected. The cloud Security association recognizes some risk in cloud computing, neglect and dishonest using of cloud computing, malicious insider, vulnerabilities, data leakage, traffic hijacking, account service and insecure application programming interface all these are recognized in march 2010. The idea came out from the conclusion that in future the concern area is key cracking and password.

In this paper [4] Duncan *et al* said about the insider attackers. That's how they attack and what are the procedures to be safe from them. Malicious insider in known by every computer security industry. Whenever companies aquire any employee related to security as a system administrator or IT security specialist so the companies seek references, check family background and take interview from him so many times. But there is a high security check on that employee. But when a company employs a service provider there is a little information

In this paper [1] the author Gruschka et al said that there are still so many security risks for users which uses the services of cloud computing. In Order to handle these hazards there must be some suitable categorization for attacks on cloud computing. In this paper the author offering one such idea of Attacks surface of the cloud computing in the detail. Now a day's one of the glorified innovations in the computer world is cloud computing. So many organizations are giving the cloud services according to the cloud computing categorization. Still, cloud computing is not full-grown and the most important thing for the user is security. In the coming age of cloud computing we assume that there will be ay new security issues between cloud computing organizations and users. We see in the new research of cloud computing there is more stress on privacy and security in new categorization attack surface about the staff and management of the provider. But in cloud computing there is a secondary provider which is used by the cloud which is not known directly by the client. In all these check which a company has on their employees there are still vulnerabilities that a trusted employs become insider attackers. A report given by the IDC that cloud based IT spending is raised by 2% in 2011 and it will be raised to 20% in 2015 so 10% of the information will be stored on cloud at that time. There will be a faith on the cloud provider by the costumers and data owners that our data is protected and safe and sound on a cloud. One of the most well-known reason why organization uses cloud computing is due to best security infrastructure. The report given by ENISA in 2009 gives the list of most significant classes of cloud definite risks. There key reason is financial gains and it is the bid revenge it is the example of the banking industry. It can also be motivated by some other reasons.

In this paper, we will also talk about Advanced Persistent Threat (APT). It was first used by the Us Air force to discuss the attack characteristics of a civilian corresponding item. But the best definition was provided by Bejtlich and command Five in cloud APT is of particular concern. Suppose the attacker attack on the host operating system, it can spread to some other virtual machine.

In this paper [5] Karnwal *et al* said that cloud computing is the grouping of distributed system, grid and utility computing. All these are combined in the form of virtualization with cloud. Due to cloud computing desktop computing is converted to server based computing because cloud computing has a huge database at the data center. Cloud computing gives a lot of advanced services which are dynamically scalable and competent. New technology of Cloud computing in the form of distributed computing system which change the entire business on the internet and give the new way to the business. SaaS was a dream which becomes true.

Cloud also provides different services like IaaS and PaaS. But all these services are provided with the help of web servers. Cloud and web servers are interdependent of each other. Web services are core services of cloud computing. On web services, cloud provides business services. All services are provided to customers are at Conceptual level cloud provider take care of all interior composite responsibilities.

The customer feels very relaxed with cloud computing. But as the nature of law when the facility in an environment increases the vulnerabilities also increases and is the same perception is in a cloud environment. As the facility is from customers it can also be used by attackers. In cloud services like SaaS, PaaS and IaaS there might be some soft corners from which an attacker can launch an attack. In SaaS scenario the attacker can attack due to the loophole in the programming interface as the insecure application programming interface (API) attacks on customer browser, firewall, and account can be hacked. So there is an attack on integrity, confidentiality and availability.

In PaaS the in secure application programming interface, unknown risk profiles and at the end this is attack on integrity, confidentiality and availability. In IaaS the main soft corner for the attacker is data leakage in virtual machine due to shared technology issues and at the end this is attack on integrity, confidentiality and availability. So for these vulnerabilities this paper focuses on SaaS layer and application programming interface security. The cloud has their own API for cloud customers to use. The intention of this paper is that open application programming interface can be protected from HTTP, XML or REST based denial of service attacks. If the cloud system is down with the attack of XML and HTTP based DDoS attack, it is more hazard than typical DDoS attack. Because these are the core protocols for cloud computing and without it there is a lack of defense. An attack on a virtual environment is different

from attack on physical systems. Hop count filter is for counting the number of hops, which are taken by the massage. It calculates the value from time to live value, there is initial and final time to live value. The final can be subtracted from an initial time to live value so the hop count can be calculated as. Hop Count = TTLf – TTLi

In this paper [6] the Liu et al is telling about wireless Local Area Network Security. WEP and WPA encryption protocols are very common it have some weaknesses. Predictive judgment is an attack algorithm which is tailored to the atmosphere of cloud computing. As compared with other platform in the attacking scenario the cloud computing is the severe hazard for wireless local area network security. The wireless local area network utilizes wireless path as a broadcast medium and the technology used for information sending and receiving is radio frequency.

With the passage of time Wireless network is going to become a very significant part of the computer network. If we compared the wireless network with wired network it can be easily extended and no more need of physical structure as we can do in wired networks. But security is the main issue the wired security is much more superior to wireless network security. The wireless network has security issues of identity cheating, eavesdropping and message tampering. IEEE 802.11 is standardized and proposed standard for wireless network it is for identity verification and data encryption it makes the wireless network more secure and enhanced. The development of cloud computing is of distributed, grid, parallel, utility computing, load balance, virtualization and network storage technology.

Cloud computing gives facilities to end user as platform as a service, infrastructure as a service and software as a service for low cost computing in large network system. The main idea of cloud computing is to decrease the load of processing on end user due to improved processing capability and on user demand the cloud computing can be used. Users have no concern with cloud internal infrastructure. The cloud server manages all the computing and storage of user data. For accurate and useful function of the system the cloud presents a range of security mechanism. Incredible computing power is given by Cloud computing. Some encryption technology has been defined by the IEEE 802.11 standard, which gives protection to data transmission.

There is integrity of data it is authentic and encrypted. WPA wired equivalent privacy is from the IEEE 802.11 WPA relates to data encryption technology, it is of high standard and gives a good security level as of the wired network. RC4 is an algorithm used for wired network security. It is nonlinear and of high level it has 10 time more speed than DES. It enlarges short key of a user to a particular extent N bit stream. RC4 is made of two algorithms Key Schedule Algorithms and Pseudo-random Generation Algorithm. It is used for building sequence related key as a stream cipher of code disk. Sequence S length is generally 256 bits. Key is private and sequence is set first for the whole procedure. And then disorder it depends upon value of key. WPA Wi-Fi Protected Access is an advanced version of WEP in IEEE 802.11-2004. It uses 128 and 48 bits key. There is a dynamic change in WPA and it is its huge development. In this paper [7] Kholidy et al discussed about the cloud intrusion detection dataset and masquerade attacks on cloud computing. Masquerades attack is one of the most serious attack for cloud system because of having huge amount of resources.

We will discuss the components and architecture of log analyzer and correlator system. Cloud computing is having some different types of attacks other than traditional IT solutions have. All these applied to SPI model of cloud computing because we have neglected and immoral use of cloud computing and have a malicious insider in our cloud environment. Masquerade attacks are related to these threats. Like when an attacker presumes the identity of a real legal user and misuse the resources.

This is the most critical attack because it has only to have information of user password. Misuse can be detected by a statistical approach to determine the action of an attack. From host based user profiling detection solutions are based. In a cloud system for detection of masquerade attacks, some techniques are used which are sequence alignment techniques, semi global alignment technique. The capability of exploiting separate sequence of audit data is one of the most important advantages. For the improvement of some technique the (HSGAA) Heuristic Semi Global Alignment Approach is developed.

It is to calculate the finest alignment present session to the same user training sequence. HSGAA approach is applied to the Cloud Intrusion Detection Dataset. Masquerade damage is based on host based user profiling. Masquerade attacker act like a legal user and breach the account of user. All the security parameters like firewalls or some security protocols are worthless because the attacker act like a legal user. But we can understand the actions of masquerader by tampering with secret information and deletion of some serious resources, using copy illegally software, eavesdropping and spoofing other users etc. and social engineering. Many of the attacks leave some log files which are directly linked with user log analysis and host based IDS used for detection mechanism.

All detection techniques which are based on analysis of user inspection. The audit or inspection is done in a different environment by several profiling methods. For example Windows, UNIX or network surroundings. In a UNIX environment user command list program and system calls can be used for audit. Seven approaches which based on UNIX commands. All these approaches are compared using same user data sets. This is an attack by simulated masqueraders. In windows environment the log sources are three applications, system and security.

Windows application and windows operating system correspondingly use system and application log sources. Local Security authority subsystem service (lsass.exe) writes to security log directly. Every event is logged fall in some category. Like directory service access, account management, object access, logon events, privacy tracking, policy change and system events. Windows environment is addressed very less in research work. Masquerades detection in network atmosphere considers user network behavior. Basic network statistics are used to detect masquerade in a network. Because host data is not reachable sometime. Legal check prevents the data access. In this paper [8] Riquet et al

discussed about coordinated attacks on a large scale and on cloud what is its impact. Firewalls and intrusion detection system are also discussed. Large volumetric data is processed by Cloud computing and it need high-quality security. Data confidentiality and protection of resources must be provided by cloud computing. Cloud security system prohibits the resources and authenticity of data from attackers. Some time in cloud computing it seems vulnerable while confront to the huge level coordinated attacks. Coordinated attacks have an impact on cloud computing and its safety solutions.

Firewalls and Intrusion Detection System are used for security using port scan. As we know that the most popular model is cloud computing, which process large volumetric data. Different services are provided by cloud computing, which are mostly used by the customers like in application software as a service, platform as a service for operation of the application and without buying and managing the costly hardware and infrastructure as a service in the form of virtualization environment and storage huge amount of data and also networking and customers' needs are fulfilled. Some more characteristics of cloud computing are load balancing, virtualization management, security and fault tolerance. But the most important concern about cloud computing is security because all cloud customer's stores confidential data on cloud servers and for security two main components are firewalls and intrusion detection systems.

Firewall is basically placed between two networks and all traffic passes through it. The authorized traffic defined by the security policy is filtered through firewall. Debar says that to detect the insecure state and usage of te system is monitored by intrusion detection system. Data integrity and application accessibility have to be assured by cloud security and it the end worms spreading, huge coordinated attacks and DDoS in prevented by Intrusion Detection System and firewalls.

In this paper [9] Khorshed et al discussed that a survey is conducted on a cloud computing to inspect those gaps that slows down cloud adoption and risk remediation challenges. And the author gives an approach of some attack types, which are machine learning techniques. Some additional tools are used to protect from these known and unknown attacks. Cloud computing is presented as "computing as utility" in the real word. Computing as utility with a huge prospective emerged in the market. It provides services on demand to customers, platform, software and infrastructure services. With the help of this setup the organizations have no need to plan their IT infrastructure in advance, this is a clear plan to develop a scalable and immediate access features setup for any organization. But there is a serious problem with the security.

Cloud computing is the most important infrastructure in the present time but in the field of security a lot of work is still needed to reduce the gap. We will spot some threats; in cloud computing threats are created for cyber-attacks, and will give some machine learning techniques for detection of threats. Some top attacks are discussed in this paper. Some top threats to cloud computing was presented by Cloud Security Alliance in March 2010. The main idea was to help the cloud users and cloud provider in identification of threat weather to join in cloud infrastructure or not and how to protect from these threats. Abusive use of cloud computing is a threat, cloud provider is restricted from instance monitoring by privacy laws. Insecure application programming interface is also a threat; malicious insider is also a threat, for recruiting the employee, many of the company policies are hid by the provider.

PROBLEM STATEMENT

From the literature review, we know that the cloud environment is unsecure because cloud is hosted on internet and always available. It makes the cloud infrastructure and attractive target.

In Cloud Environment user are authenticated with different mechanisms for web services. Different companies use different techniques and mechanisms for authentication propose. These authentication techniques and mechanisms can be vulnerable if their IT technical are not professional to avoid this overhead authentication process can be handed over to some other company providing excellent authentication services after signing SLA (service level agreement) with the said company.

IMPLEMENTING USER AUTH AS SERVICE FOR CLOUD NETWORK

In initial setup of hosting the web services there are web services, FTP and data sharing etc. But in this model the main issue was the direct assess of different resources which is not a good approach in this approach the companies only focusing services availability, but not focusing on the secure / strong users' authentication.

Same issue here in mail services, storage service, etc. Company should focus on strong /secure authentication too. Inside design your initial build for hosting regarding various services was they provide world-wide-web services FTP and also information sharing. Although there is difficulties in the actual model which they simply just emphasizing on availability mostly hosting companies only focusing on their service availability, but in our model we also focused on as well as the availability together with secure authentication. The main issue in actual model was the direct accessibility which is a security issue, we suggested that there should be a cloud gateway and authentication/ source selection which is a web interface provided by the service provider.

Here every user will be authenticated, after that the user will be allow to the desired and have the access of the specific services, but if did not provide authentication the access will be denied. Here the secure authentication mechanism is applied with the help of cloud gateway and authentication server as shown in Fig 1 and 2. Identification fraud remains significant well-known difficulties on the internet these days. Reports point out that will digital identity illegitimacy remains happening more often. Using the upward pattern of shifting data and services into the World wide web along with cloud-based programs, the particular management along with control of entry to private along with hypersensitive data has grown a lot more than making sure easy end user references for the onset of end user periods for example software, sufficient reason for higher interconnectivity along with interdependencies between multiple apps, products and today involve, throughout additional generalized words, various sorts of enhanced shared-secret or multifactor strong authentication. AaaS gives up every one of the regular SaaS great things about scalability and also outsourced experience.

AaaS not just gives stability and functional positive aspects, but this may also supply a distinguishing side regarding very sensitive devices.

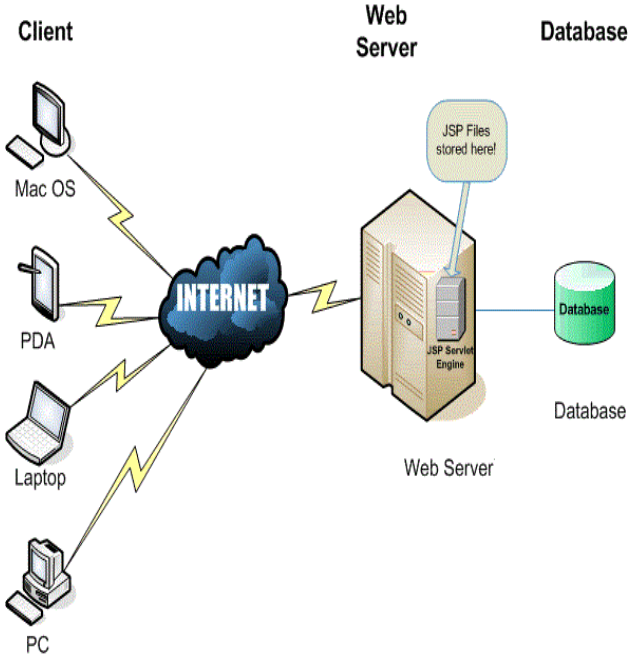

Fig 1. Suggested model

actually used mainly through a browser that's limited access to your surroundings and devices (computers, PDA, IPad) etc.The most common solution strategies that are employed

Because authentication strategies modify, AaaS furthermore provides a smoother improve route to maintain while using newest strike developments. Numerous on premise programs have got suffered with undesirability, however, are very costly in addition to too ingrained inside the IT fabric to improve easily of which alterations while shifting to a providers startup. But similar to any kind of brand-new deployment design, AaaS is just not without the difficulties. Among the complications Older considers clients experience is thinking which services like individual sign-on (SSO) AaaS offer a fairly easy shortcut to obtaining identities inside foreign not too, he / she states that, detailing that all the basic principles keep a similar. First, we take core i3 laptop. We put 8GB RAM and install 64 bit operating systems. Then we install the VMware workstation 9. It is 64 bit operating systems. We create machines on that VMware and install operating system just like we install the operating system on the physical machines. When we install the VMware on a machine, that machine is called the host machine. The machines which are created on the on the VMware are called the guest machines.

There are different states of the VMware for example, we can suspend, resume, power off, power on, and restart the machines created on the VMware. First of all we created a machine on VMware and give 1GB RAM and the hard desk 40 GB. Then install the window server 2008R2 on that machine. Window server 2008R2 is 64 bit operating systems. First, we install the VMware tools because without the installation of the tools we cannot do any work on that machine.. After this we have to create two machines on the ESXI server. So we cannot do that work directly on the ESXI server. We install the Vsphere console on another machine and create the proposed machines on that client. But this machines are actually made on the ESXI but virtually we see that this work is done on the client. so for the creation of these machines. Put there IP address of the same range. From Vsphare we can manage the ESXI server.

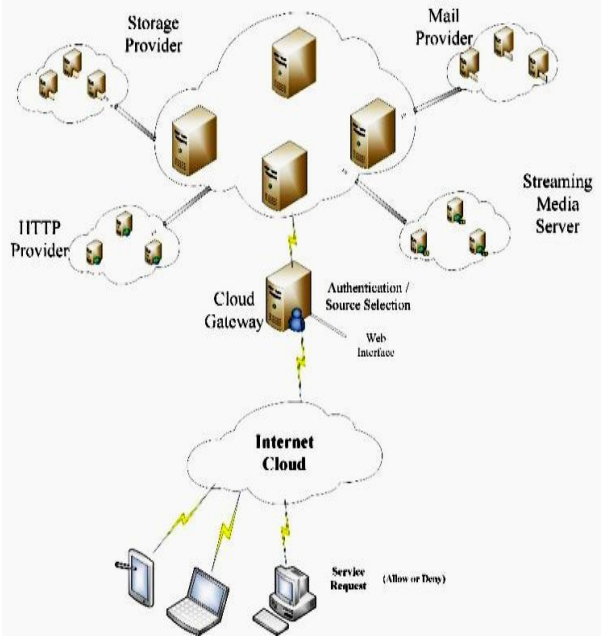

Fig 2. Suggested model in detail

Then we create the two machines on the ESXI through the use of Vsphare. The ESXI is just like dos window. It is control and manage from this vsphere. If we do some work or store some data on this client. Virtually we see that it is store on the client, but it is stored on the ESXI server. If we want to add or remove some data or machines from the ESXI it is also done from that client. Then we create another machine and give the resources of 160GB hard desk and 4 GB RAM. And install the ESXI server on that machine. Now, according to our model we have to create two machines. One have window 7 and on the other window XP is installed. So we do not do directly on the ESXI. Create the suggested machines on that client.Then we create a third machine on the VMware and give the resources of 30 GB hard desk and 1GB RAM and install the window 7 on that machines.

TESTING AND EVALUATION

In our model we have many servers on which the cloud services are hosted. There are many virtual machines which are made on that cloud. These virtual machines work just like physical machines and use the resources of the host machines. The machine which creates the virtual machine are called host machine and the operating system installed on that host machine is called a host operating system shown in Fig 3 and 4. The virtual machines which are made on the host machine is called the guest machines and the operating system install on that virtual machines are called the guest operating system. So these guest machines work just like host machine and use the resources of host machines. When we do some work on that virtual machines. So virtually we see that the work is done on the virtual machine but actually that work is done on the cloud and also save on the cloud. In our

cloud model, there are many services, to which we provide the secure authentication services are, storage provider, http provider and video audio streaming provider. In our model the user send the request from his device that can be a laptop, PC or IPad etc. That get access through the internet cloud, and reached to the cloud gateway, where the authentication server is placed, it is a web interface. The legitimate users are authenticated and the desired services are provided if the user proved their identity to that authentication server. The user has to provide the correct user name, password and a captcha. After the successful authentication the user is going to access the FTP service, by providing the user name and password.

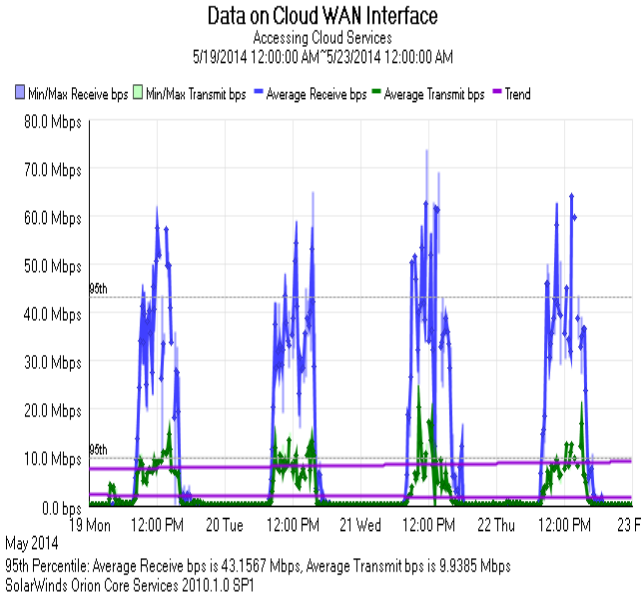

Fig. 3 Data interface on cloud WAN

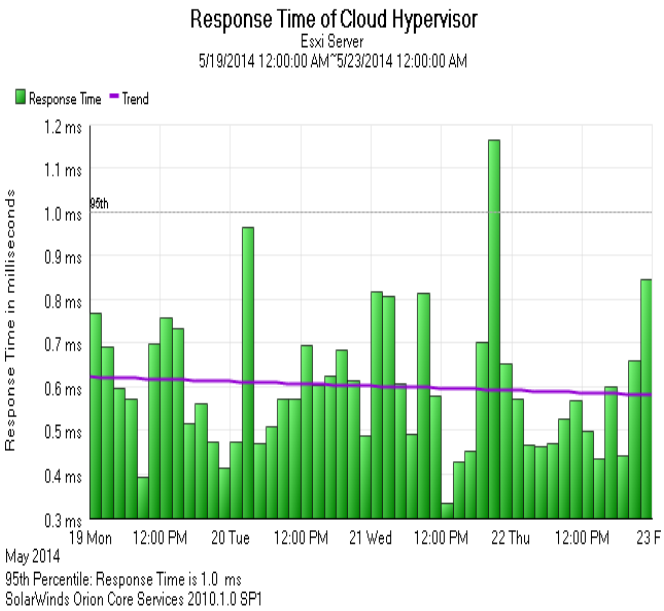

Fig 4. Response Time of Cloud Hypervisor

CONCLUSION

Results show that model works perfectly in suggested environment, response time was calculated and high data transfer was tested to evaluate performance of the model. It only requires high speed bandwidth to transfer data from service providing cloud company to authentication, providing cloud company because user will not be able to access cloud services directly as in traditional approach.

REFERENCES

[1] Gruschka, N., and Jensen, M, "Attack Surfaces: A Taxonomy for Attacks on Cloud Services", IEEE 3rd International Conference on Cloud Computing, 2010, pp.276-279.

[2] Stolfo, S, J., Salem, M, B., and Keromytis, D, A, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud", IEEE CS Security and Privacy Workshops, 2012, pp.125-128.

[3] Yang, L., Zhang, T., Song, J., Wang, J., and Chen, P, "Defence of DDoS Attack for Cloud Computing",IEEE International Conference on Computer Science and Automation Engineering (CSAE), 2012, pp.626-629.

[4] Duncan, A., Creese, S., and GoldSmith, M, "Insider Attacks in Cloud Computing", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communication, 2012, pp.857-862.

[5] Karnwal, T., Sivakumar, T., and Aghila, G, "A Comber Approach to Protect Cloud Computing against XML DDoS and HTTP DDoS attack", IEEE Students' Conference on Electrical, Electronics and Computer Science, 2012, pp.1-5.

[6] LIU, R., and LI, J, P, "A Predictive Judgment Method For WLAN Attacking Based On Cloud Computing Environment",2010 International Conference on Apperceiving Computing and Intelligence Analysis (ICACIA), 2010, pp.22-25.

[7] Kholidy, H, A., and Baiardi, F, "CIDD: A Cloud Intrusion Detection Dataset For Cloud Computing and Masquerade Attacks", Ninth International Conference on Information Technology – New Generations, 2012, pp.397-402.

[8] Riquet, D., Grimaud, G., and Hauspie, M, "Large-scale coordinated attacks: Impact on the cloud security", Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2012, pp.558-563.

[9] Khorshed, M, T., Ali, A, B, M, S., and Wasimi, S, A, "Trust Issues That Create Threats for Cyber Attacks in Cloud Computing", IEEE 17th International Conference on Parallel and Distributed Systems, 2011, pp.900-905.

[10] Sqalli, M, H., Al- Haidari, F., and Salah, K, "EDoS-Shield – A Two Steps Mitigation Technique against EDoS Attacks in Cloud computing", IEEE International Conference on Utility and Cloud Computing, 2011, pp.49-5.