International Journal of Grid and Distributed Computing
Vol. 9, No. 10 (2016), pp.197-210
http://dx.doi.org/10.14257/ijgdc.2016.9.10.18

Implementation of User Authentication as a Service for Cloud Network

Masood Shah[1], Abdul Salam Shah[2*] and Imran Ijaz[3]

[1,2,3]*SZABIST, Islamabad, Pakistan*
[1]*engg.cisco@gmail.com,* [2]*shahsalamss@gmail.com,* [3]*imran-ijaz@live.com*

Abstract

There are so many security risks for the users of cloud computing, but still the organizations are switching towards the cloud. The cloud provides data protection and a huge amount of memory usage remotely or virtually. The organization has not adopted the cloud computing completely due to some security issues. The research in cloud computing has more focus on privacy and security in the new categorization attack surface. User authentication is the additional overhead for the companies besides the management of availability of cloud services. This paper is based on the proposed model to provide central authentication technique so that secured access of resources can be provided to users instead of adopting some unordered user authentication techniques. The model is also implemented as a prototype.

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

1. Introduction

The cloud computing provides centralized security for data and processes and high availability, but it has so many security challenges that can cause a huge loss to an organization in the form of degradation [1]. The cloud computing is mostly used as application software as a service and platform as a service for the operation of the other applications. The cloud provides services to users without buying and managing the costly hardware and infrastructure in the form of virtual environment [2]. The users can store the huge amount of data and get the benefit of the networking services with load balancing, security, and fault tolerance. The cloud customer's store confidential data on the cloud so for the security of the servers, firewall, and intrusion detection systems are important [3].

The cloud security association recognized some risk in cloud computing, as neglect and dishonest usage of cloud computing, the malicious insider, vulnerabilities, data leakage, traffic hijacking, account service and the insecure application programming interface [4]. The data confidentiality and protection of resources must be provided by the cloud computing. The cloud security system prohibits resources and authenticity of the data from attackers [5].

Types of cloud computing include public, private, and hybrid cloud. In public cloud, services are public and accessed through the public network. In the private cloud, private services are accessed through the private network and the combination of public and private services is known as the hybrid cloud. The services provided by the cloud are categorized as the SPI. The layers of the SPI model are SaaS, PaaS, and IaaS. The general architecture of the cloud is the authentication server, the user, and server [6-8].

* Corresponding Author

ISSN: 2005-4262 IJGDC

The remaining paper is organized as; in the section 2 Literature Review is provided, section 3 contains Problem Statement, section 4, contains Traditional Approaches, Proposed Model is provided in section 5, and following that the Implementation is provided in section 6, section 7 contains Testing, Evaluation and Results, and finally in section 8, the Conclusion of the study is provided.

2. Literature Review

According to Gruschka *et. al*. [9] cloud computing has three different contributor classes which are the user, the cloud, and service. The cloud has three basic models that are IaaS, PaaS, and SaaS. The most well-known surface attacks in cloud computing are server-to-user attack and most common attacks are buffer overflow attacks and SQL injection. The SSL certificate spoofing or Phishing attacks on mail clients is also common in the cloud. Another type is triggering the cloud provider or denial of services. The next attack surface is user-to-the cloud provider common attacks on this surface is Phishing attacks which cause a user to control the cloud provider services. One of the attack surfaces is cloud to service. The cloud organization integrates every kind of attack beside the running service on the cloud. One of the drawbacks found in the control system service which uses a Signature Wrapping attack has the possibility to alter eavesdropped message, although it has a digital signature. The client and server cannot communicate unless the server authenticated client. During communication, the hash function is used for the integrity of the data and stopping different attacks. The authentication is once again required if the user wants to access the new services on the cloud. The denial of services attack is possible in this method by sending the repeated request to the server by the unauthorized user, the man in the middle and brute force attacks are also possible.

Stolfo *et. al.*, in [10] used decoy technology to supervise and sense unusual data access. Suppose when an illegal access is detected and confirmed so the system produces a large amount of decoy data for an attacker to cut off his access to the real user data. According to the security Alliance, the top threat for cloud computing is when the attacker is the malicious insider and majority of the user know the threat. If a hateful insider allowed someone outsider to access your password key or your personal data is another threat. The fog computing uses decoy information for the prevention of attacks. The other use is the online social network by a separate user. User behavior profiling is a method to monitor the access of normal user that how many times and when the users access the data in the cloud. The authors have used behavior profiling and decoys for securing information. By using decoy information, we put honeypots and other fake data can be produced to detect the illegal entry to the cloud. The decoy information will puzzle the attacker and then he will not understand the original and fake information that is honey pots. Invader is puzzled with fake information. The architecture specified in this paper is easily implemented in Cloud (Suggest-File System). User behavior Profile and Decoys together gives high-level security. By using the specified methods mention in the paper there is less possibility of the attack. In the authentication process, a man in the middle attack is also possible. The attacker can get useful information from the data transmitted between the trusted authority and the hardware. The masquerade attack is possible in the registration process.

Yang *et. al.,* in [11] described DDoS attacks and the mechanism that how to recover or trace back the attack. Basically, the DDoS attack on the availability of cloud services. The defensive techniques for DDoS attacks are detection, identification, and filtration. For the detection of the DDoS attack, wavelet spectral analysis, statistical methods and machine learning are used. The IP Trace-back, probabilistic packet marking (PPM) and Deterministic packet marking (DPM) techniques are used to identify the attack source in identification phase. The PPM needs a reduced amount of traffic than ICMP to rebuild the path to recognize the attack source, but it requires additional calculation and packets for the trace-back procedure. The SOA-Based Trace-back Approach (SBTA) is used to

trace back the actual cause of DDoS attack in the cloud. The SBTA scalable, flexible and compatible. The infected client can recover his cloud by the trace-back tag and can find the place that from where the attack is launched. There SBTA used advanced packet marking based on CEFS to find out path restoration. For the defense against DDoS attacks the traffic control mechanisms known as ingress and egress filtering are used. The other most advanced method, StackPi, is used to insert a digital signature in IP packets to prevent the Spoofing of the source address.

Duncan *et. al.*, in [12] discussed the insider attacks. The Insider is anyone who has the authorized access to the organization's network or information system. The computer in the home is shared between family members, but for a cloud user it can be malicious. The data and resources can be spoiled by a family member who might innocently or accidently mutate the information or system. In the family, many children have more knowledge than their parents and it can harm your data by the full access to the resources by your cloud account by viewing all the web content, password hacking or cracking or downloading the restricted thing without leaving history are the several misuses. A friend or family member become more malicious when there is an optimist feeling in the relationship.

Infrastructure as a Service basically runs the hypervisor and it manages many operating systems in the virtual machine on the host operating system, the customer has no concern that which virtual machine runs on which server. But there is an impact on security because the customers have no idea that how many copies of his virtual machine exists, where the located position is and who access it. It is possible that the malicious insider takes the copy of the customer virtual machine and takes it to the outside hypervisor, but it depends on the cloud provider. The malicious insider can break the administrator password and can access all the data on the customer virtual machine and obtain a complete history of the virtual machine.

Riquet *et. al.*, [13] discussed Firewall, intrusion detection and coordinated attacks on the cloud on a large scale. The authorized traffic defined by the security policy is filtered through the firewall. The most common techniques used for detection are the anomaly-based detection and pattern matching. The anomaly based detection allows all normal traffic, an alarm is raised when deviation from normality is detected, but there is a chance to raise a false alarm. The IDS cannot detect those port scan attack which is executed with a very slow speed rate. The security solutions are Snort and commercial firewall. The Snort is an open source IDS, to analyze the network, and traffic in real time. The other solution is Commercial firewall.

Khorshed *et. al.*, in [14] proposed an approach based on some machine learning attack types. In cloud computing threats are created for cyber-attacks. The data loss, account service, and traffic hijacking are threats. For hybrid clouds, digital identity management is not enough, in a present way. In unknown risk profile the lake of transparency, for audit logs are provided unwillingly. The model has focused on the detection of attacks during the start or when an attack is occurring. The model informs the user that what kind of attack is happening. The machine learning techniques has been used, for the known attacks. The machine learning technique takes the proactive action to solve the problem, if the attack exists. The machine learning technique also inform the owner of the data and the security administration about the known attacks. The performance information is available to cloud clients and evaluating the attack by this data will complete both. The Defiance of its functionalities attacks; Dangerous internal attacks; Shared Memory targeted by attacks; and Phishing attacks are possible in the cloud environment.

3. Problem Statement

The cloud environment is unsecured because the cloud is hosted on the internet and is always available that makes it an attractive target. In the cloud, users 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 not dealt by trained IT professionals. The overhead of the manual authentication process can be handed over to some other company providing excellent authentication services after signing a Service Level Agreement (SLA) or dealt by IT professionals with the proper authentication method. To solve the authentication problem we have proposed a model which is basically a modification of the already-proposed models.

4. Traditional Model/Approach

In the initial setup of hosting web services, there are three basic components, *i.e.*, Web Services, File Transfer Protocol (FTP) and Data Sharing. The main disadvantage of the traditional model is the direct access to different resources [15]. The companies only focusing on service availability, and not on the secure and strong user authentication. The issue is same in mail services and storage service. Companies should focus on strong /secure authentication along with the service availability. The traditional model can be seen in Figure 1.

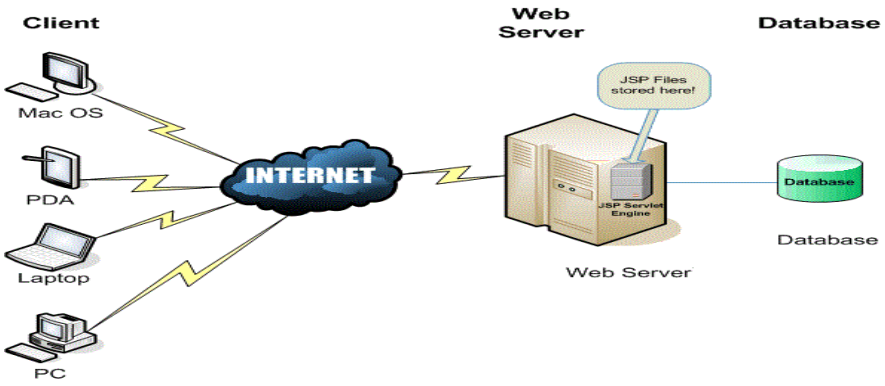

Figure 1. Traditional Model

5. Proposed Model

The traditional models emphasize on the availability, but the proposed model focus on the secure authentication along with the availability of cloud services. To avoid direct accessibility of resources, there should be a cloud gateway and authentication / source selection as web interface provided by the service provider. The user will be authenticated, and after, that the user will be allowed to use desired services with the access of specific services only. If the user failed to provide authentication the access will be denied [16]. In the proposed model the secure authentication mechanism is applied with the help of the cloud gateway and the authentication server. The identification fraud remains significant well-known difficulties on the internet. The significantly exploited approaches are increasing associated with accounts access by means of obtaining reusable qualifications regarding the sites that have not applied strong individual authentication [17].

Several assaults are usually demonstrated while Phishing messages that masquerade with versions. They might be routed by simply genuine corporations and also consist of URL that point for you to fake Internet sites which may have

exactly the same performances like legitimate versions [18]. The proposed model concentrates on approaches which might be utilized to put into action secure authentication for the user with regard to online user identities. The item looks at useful remedy approaches, overall architectural mastery design, and promising developments. Secure End user Authentication So, how must all of us increase Web-based user authentication techniques without compromising usability and ubiquity, once the Web is actually used mainly through a browser that's limited access to your surroundings and devices [19-20]. The most common solution strategies that are employed today involve, throughout additional generalized words, various sort of boosted shared-secret or multifactor strong authentication. The proposed model is provided in Figure 2.

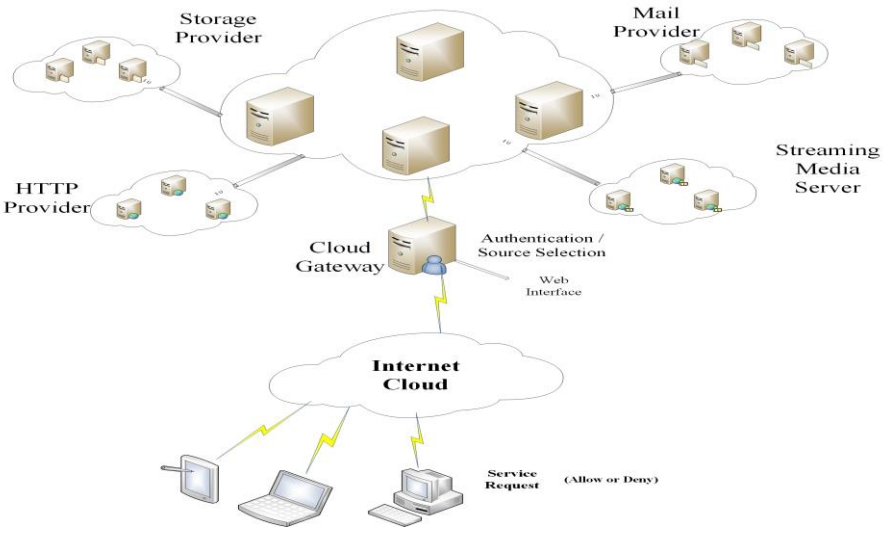

Figure 2. User Authentication as a Service for Cloud Network

6. Implementation of the Model

For the implementation of the proposed model following procedure and tools have been used.

6.1. System Requirements

The Intel core i3 laptop having 3.00 GHz processor and 8 GB RAM has been used for the implementation of the proposed model. For creating the cloud environment and the installation of VMware Workstation 9, Windows 7 (64 bit) operating system has been installed.

6.2. VMware Workstation

The VMware is a computer software which provides services similar to a physical machine with an operating system and applications. We have installed the VMware workstation 9 on the 64bit host operating system, which is running on the physical host machine. We have created three virtual machines so that window 7, window server 2008 and ESXI operating systems can be installed on each machine. These virtual machines use and share the resources (hard drive, Ram) of the actual physical machine. The user can run these machines at the same time, so we have now three virtual and one physical machine. The states of VMware can be saved for the backup and recovery using snapshot function provided by VMware software.

The snapshot helps in recovery in case of crashes or other problems. The user can easily recover the system to that state for which a snapshot has been taken.

6.3. Creating new Virtual Machines

As per requirements, we have to create three virtual machines with the help of the wizard window. The wizard provides options of the typical and custom installation. The typical installation selects the components automatically and less overhead is involved, but the extra components consume more memory. The installation process provides an option to install virtual machine along with the operating system or without an operating system. In the first step, three virtual machines have been created and in the next step windows 7, Window Server 2008 R2 and ESXI Servers have been installed.

6.4. Installation of VMware Tools

The VMware tools is a package of drivers and software for the better performance of the guest machine. If the VMware tools are not installed properly the guest machine will not work as per user requirements and the user will miss the following important functions and features.

1. The user cannot perform the copy and paste operation from host machines to the guest machine.
2. The time of the guest and host machines will be not be synchronized.
3. Data sharing will not be possible.
4. The unity of the guest and the host will not be achieved.

The process of the installation of tools is very simple, the user has to turn on the desired VMware and select VM tools. The installation wizard will appear through which the user can install desired tools and restart the VMware machine which is now ready to use. The VMware has different states like, Suspend, Resume, Power off, Power on and Restart.

6.5. Installation of Windows Server 2008 R2

The installation of three virtual machines has been successfully done. The created machine is now ready for the installation of the window server 2008 R2. Window server 2008 R2 is the product of Microsoft that provides advanced features for the setup of a server. The installation of the Window Server 2008 R2 on a virtual machine requires system resources. It requires a 64-bit processor having a minimum speed of 1.4 GHz. The memory selection depends upon the user need, if we select the minimum, it provides a 512 Mb of RAM. The recommended option provides 2 GB of RAM and the maximum option provides 8 GB of RAM. The graphics requirements are a super VGA of (800; 600) or higher. The required disk space is 32 GB but if the RAM size is selected as the maximum then it required more disk space. The virtual machine has been created as per requirement of the windows server 2008 R2 so the installation has not created problems. The window server 2008, has been installed on a virtual machine having 2 GB of RAM and 40 GB of the hard disk as shown in Figure 3, and the starting of installation step can be seen in Figure 4. Still, the edit option is available if the installation of server creates the problem the user can modify the specifications of the virtual machine.

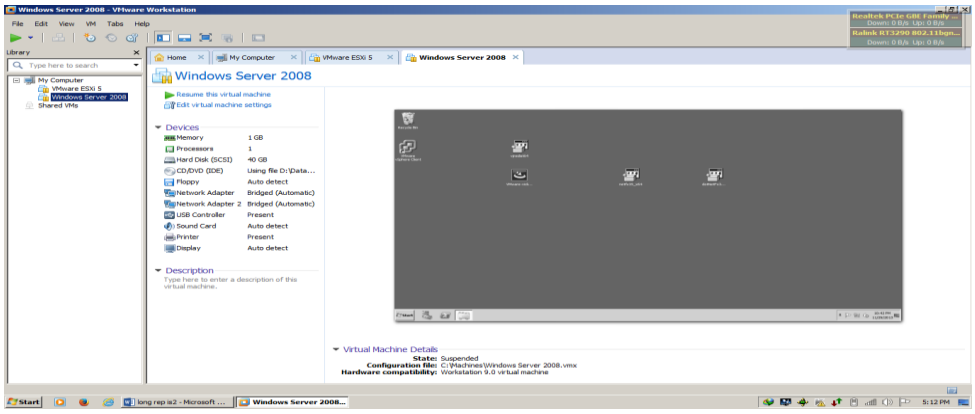

Figure 3. Specifications for Windows Server 2008

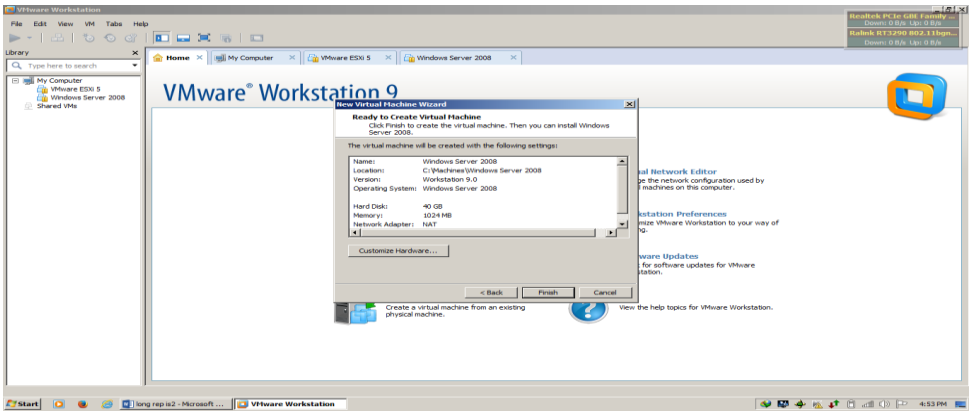

Figure 4. Installation of Windows Server 2008

The installation of the tools has been carried out so that the user can perform some tasks with Window Server 2008. The Windows Server 2008 is now ready as shown in Figure 5. If the user wants to access ESXI servicer from window server 2008 then the installation of vSphere on Window Server 2008 is also compulsory.

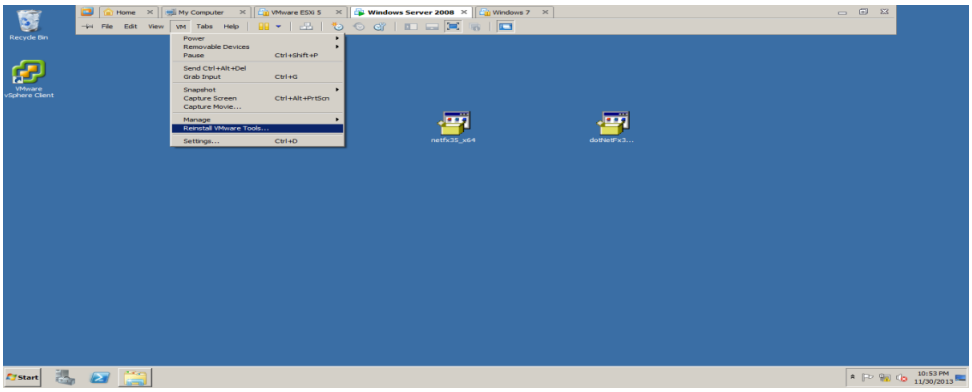

Figure 5. Virtual Machine Having Windows Server 2008

6.6. Installation of ESXI Server

The installation of ESXI server has been carried out on the already created virtual machine. The machine has a hard drive of 100 GB, and 4 GB of RAM. The user cannot perform tasks with ESXI directly, because ESXI is command based just like DOS. If the user need to perform any task on ESXI Server, an additional component

needs to be installed on a separate client machine. The installation of a console vSphere is needed on a separate machine from where the user can access and manage the ESXI server. Every task performed via vSphere will be physically performed on the ESXI.

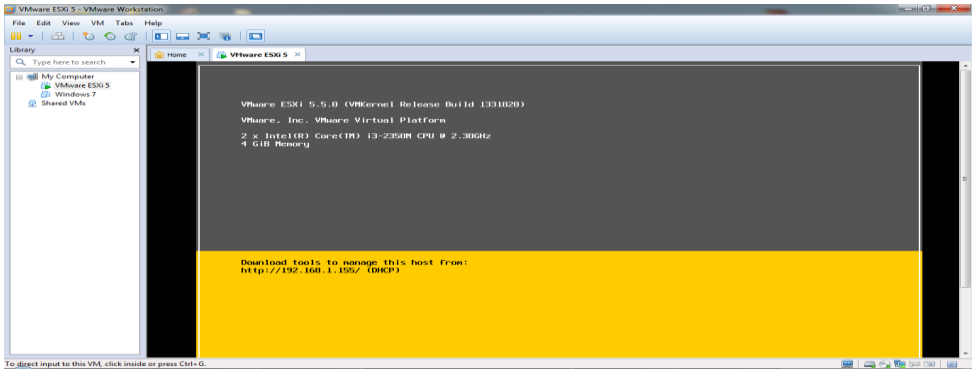

Figure 6. Virtual Machine Having ESXI Server

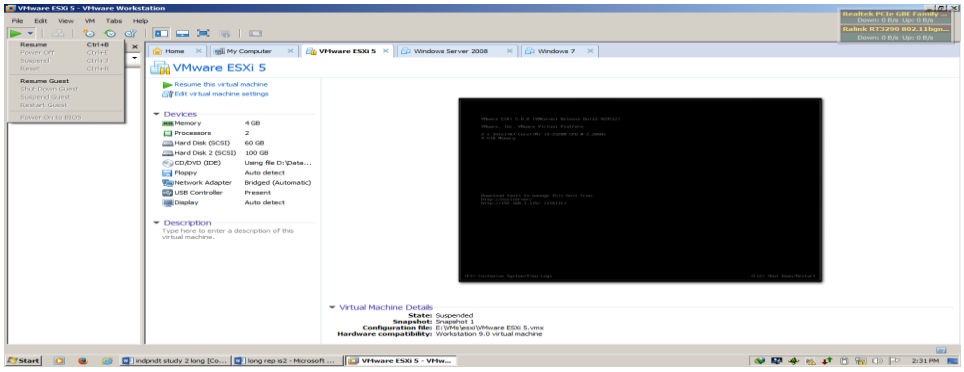

Figure 7. Specifications of ESXI Server

6.7. Installation of Windows 7 (64 bit)

The installation of Windows 7 (64 bit) has been carried out on the already created virtual machine. The virtual machine has 2 GHz processor, having 4 GB of RAM and 40 GB of hard disk space. The installation of vSphere has been carried out on windows 7 so that we can access the server. The work performed on the Windows 7 client machine will be stored on the ESXI server. The addition or deletion of data or machines from the ESXI can also be carried out using the client machine.

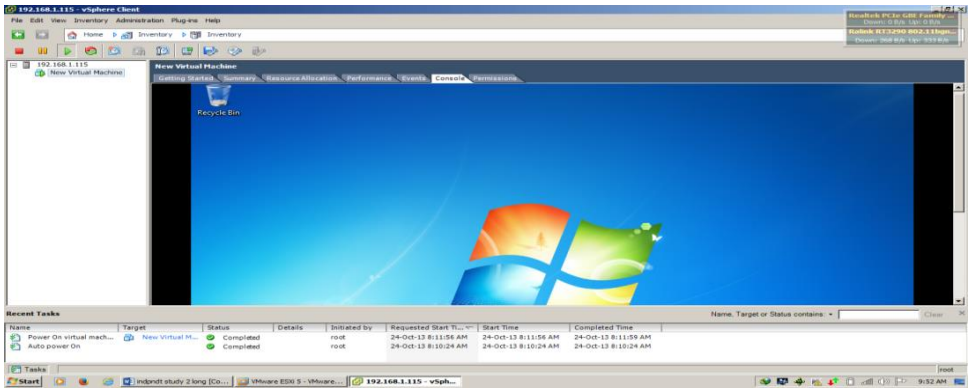

Figure 8. Windows 7 (64 Bit)

6.8. Installation of vSphere Client

The installation of the vSphere client is necessary to interact with the ESXI server and Windows Server 2008. The server cannot directly be accessed for the storage of data or for any other access to data. To access the ESXI server from the Windows Server 2008, the installation of the vSphere software has been carried out on the Window Server 2008. During the installation of vSphere a warning has been received that the installation of VJ-redist 64 is mandatory before proceeding for the installation of vSphere. The VJ-redist 64 is a visual j redistributable 64-bit software that works with only 64 bit operating systems and it supports all the server and client packages. The VJ-redist 64 has been successfully installed and resumed the installation of vSphere but another warning message has been received that the installation of Dot net 3.5 x64 is required. The installation of Dot Net 3.5 x 64 bit has been successfully carried out. The installation of vSphere has been started and completed successfully. The vSphere client can be used by providing an IP address of the ESXI server, username, and the password. The selection of the IP address of both machines from the same series is important. In a similar way if the user wants to access the server from the machine having windows 7, then the installation of vSphere on that machine is also important. So we have carried out the installation of vSphere software on the virtual machine having windows 7 (64 bit) installed.

7. Testing, Evaluation and Results

In the proposed model HTTP Server, Storage Server, Mail Server and Media Server have been created so that the cloud services can be hosted. The servers created on virtual machines work just like physical machines and use the clients can use resources of the host machines. In the proposed cloud model we provide secure authentication to the servers and services of storage provider, http provider and video audio streaming provider. The user sends the request from the device that can be a laptop, PC or tablet, to access the cloud [21-22]. The request reaches to the cloud gateway, where the authentication server is placed, which 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. In the case of wrong username and password the services will not be provided to the user. After the successful authentication the user is going to access the FTP service, by providing the user name and password as in Figure 9. The important FTP services are kept secure from any kind of loss Figure 10.

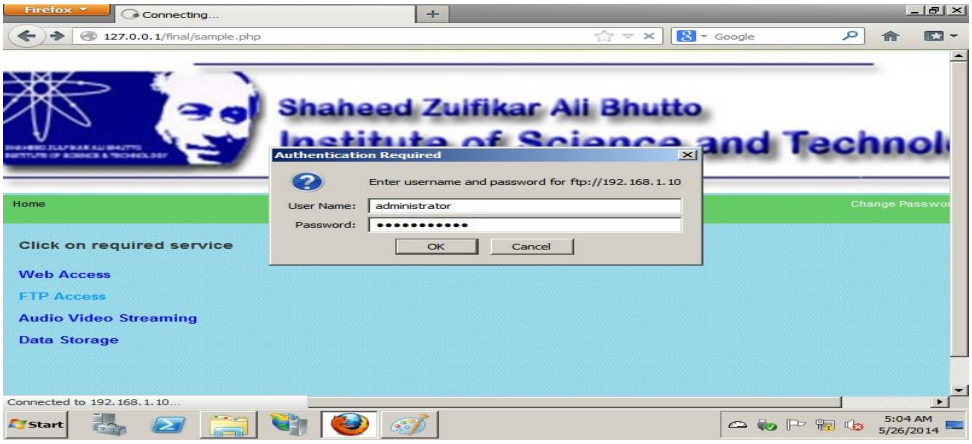

Figure 9. User Authentication

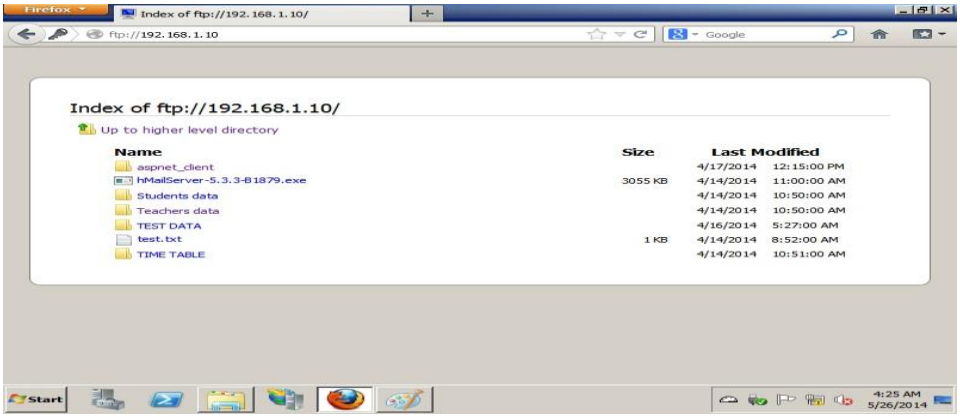

Figure 10. Secured FTP Services

For the evaluation of the proposed model, data requests have been placed and the response time has been calculated. The results shows that the model works perfectly in the suggested environment, response time was calculated and high data transfer was tested to evaluate the performance of the model. It only requires high speed bandwidth to transfer data from service providing cloud company to authentication providing cloud company because the user will not be able to access cloud services directly as in traditional approach. The results have been graphically represented in Figure 11, and 12.

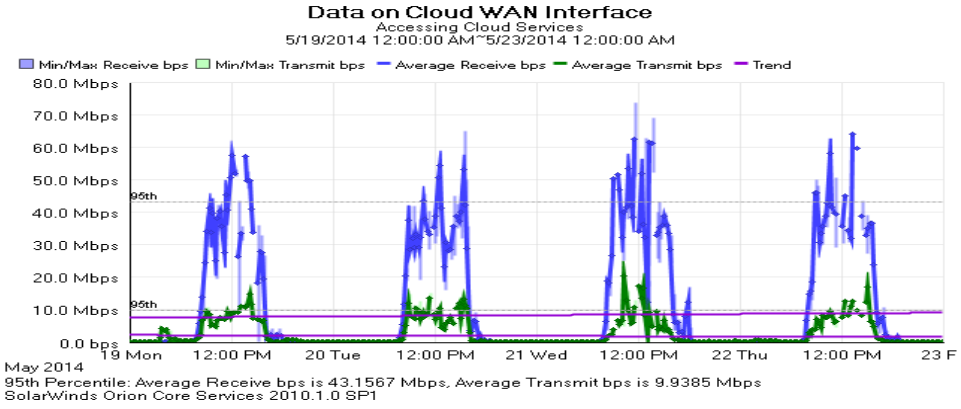

Figure 11. Accessing Cloud Services

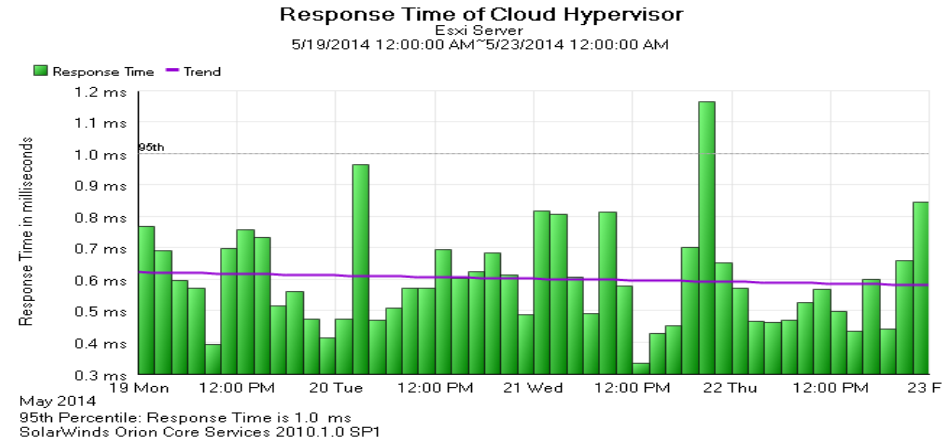

Figure 12. Response Time of ESXI Server

8. Conclusion

In this paper, a model for providing authentication to the users of cloud computing has been presented. Window Server 2008, ESXI Server and Windows 7 were installed to create the cloud environment. Data protection to the resources has been provided through a web-based authentication server. The user authentication is the additional overhead for the companies besides the management of availability of cloud services. In this paper, we have tried to reduce the overhead of the companies using cloud computing. The model just implemented as a prototype, in the future we will increase more security using signatures and add more services into the circle of authentication [23-24].

References

[1] M. Shah and A. S. Shah, "Appraisal of the Most Prominent Attacks due to vulnerabilities in cloud computing," International Journal of Grid and Distributed Computing (IJGDC), vol. 9, no. 7, **(2016)**, pp. 13-22.
[2] M. Uddin, J. Memon, R. Alsaqour, A. Shah, M. Z. A. Rozan, "Mobile Agent Based Multi-Layer Security Framework for Cloud Data Centers", Indian Journal of Science and Technology, vol. 8, no. 12, **(2015)**, pp.1-10.
[3] A. Waqas, A. W. Mahessar, N. Mahmood, Z. Bhatti, M. Karbasi and A. Shah, "Transaction Management Techniques and Practices In Current Cloud Computing Environments: A Survey", International Journal of Database Management Systems, vol. 7, no. 1, **(2015)**, pp. 41-59.
[4] M. Uddin, A. A. Rahman, A. Shah and J. Memon, "Virtualization Implementation Approach for Data Centers to Maximize Performance", Asian Network for Scientific Information (ANSINET), vol. 5, no. 2, **(2012)**, pp. 45-57.
[5] M. F. Ali, A. Bashar and A. Shah, "SmartCrowd: Novel Approach to Big Crowd Management using Mobile Cloud Computing", 2015 International Conference on Cloud Computing (ICCC), **(2015)**, pp.1-4.
[6] A.G. Memon, S. Khawaja and A. Shah, "Steganography: A new Horizon for Safe Communication Through XML", Journal of Theoretical and Applied Information Technology, vol. 4 no.3, **(2008)**, pp. 187-202.
[7] A. Shahzad, S. Musa, M. Irfan, A. Shah, "Key Encryption Method for SCADA Security Enhancement", Journal of Applied Sciences, vol. 14, no. 20, **(2014)**, pp. 2498-2506.
[8] A. Shahzad, S. Musa, M. Irfan, A. Shah, "Deployment of New Dynamic Cryptography Buffer For SCADA Security Enhancement", Journal of Applied Sciences, vol. 14, no. 20, **(2014)**, pp.2487-2497.
[9] N. Gruschka and M. Jensen, "Attack Surfaces: A Taxonomy for Attacks on Cloud Services", IEEE 3rd International Conference on Cloud Computing, **(2010),** pp.276-279.
[10] S. J. Stolfo, M B. Salem and D. A. Keromytis, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud", IEEE CS Security and Privacy Workshops, **(2012),** pp.125-128.
[11] L. Yang, T. Zhang, J. Song, J.S. Wang and P. Chen, "Defence of DDoS Attack for Cloud Computing", 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE), **(2012),** pp.626-629.
[12] A. J. Duncan, S. Creese and M. GoldSmith, "Insider Attacks in Cloud Computing", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communication, **(2012),** pp.857-862.
[13] D. Riquet, G. Grimaud and M. Hauspie, "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.
[14] M. T. Khorshed, A. B. M. S. Ali and S. A. Wasimi, "Trust Issues That Create Threats for Cyber Attacks in Cloud Computing", IEEE 17th International Conference on Parallel and Distributed Systems, **(2011)**, pp. 900-905.
[15] T. Karnwal, T. Sivakumar and G. Aghila, "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.
[16] R. Liu and J. Li, "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.
[17] H. A. Kholidy and F. Baiardi, "CIDD: A Cloud Intrusion Detection Dataset for Cloud Computing and Masquerade Attacks", Ninth International Conference on Information Technology – New Generations, **(2012),** pp. 397-402.
[18] M. H. Sqalli, F. Al- Haidari and K. Salah, "EDoS-Shield – A Two Steps Mitigation Technique against EDoS Attacks in Cloud computing", IEEE International Conference on Utility and Cloud Computing, **(2011)**, pp. 49-56.

[19] A. Iqbal, H. U. Rahman, M. U. Khan and M. Fayaz, "Secure Data in Cloud on the Basis of Sensitivity", Journal of Applied Environmental and Biological Sciences, vol. 6, no 2, **(2016)**, pp. 102-108.
[20] A. Raza, M. Y. Koondhar, Sindhu, M. Hyder, G. D. Menghwar, B. Baloch and A.Shah, "Application Service Delivery in the Modern Virtualized Data Center-Improving Reliability and Scalability", Sindh University Research Journal (Science Series), vol. 48, no. 3, **(2016)**, pp. 579-584.
[21] A. W. Mahesar, Z. Bhatti, A. Waqas, M. Y. Koondhar, M. M. Rind, and S. Nizamani, "Efficient Link Prediction Method in Dark Network Analysis", Sindh University Research Journal (Science Series), vol. 48, no. 1, **(2016)**, pp. 81-84.
[22] H. Nawaz, S. Soomro, S. H. Abbas, M. S. Ehsan and M. Y. Koondhar, "Simulation Based Analysis of Handover Issues Affecting UMTS Performance", Sindh University Research Journal (Science Series), vol. 45, no. 4, **(2013)**, pp. 689-696.
[23] A. S. Shah, M. N. A. Khan, F. Subhan, M. Fayaz and A. Shah, "An Offline Signature Verification Technique using Pixels Intensity Levels", International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 9, no.8, **(2016)**, pp. 205-222.
[24] A. S. Shah, M. N. A. Khan and A. Shah, "An Appraisal of Off-Line Signature Verification Techniques", International Journal of Modern Education and Computer Sciences, vol. 7, no. 4, **(2015)**, pp. 67-75.

Authors

Masood Shah, enthusiastic and high-achieving IT professional, has completed MS degree in Computer Science from SZABIST, Islamabad, Pakistan in 2016. He did his Bachelor of Information Technology from Agricultural University, Peshawar Pakistan in 2012. He has completed short courses and diploma certificates in CCNA (Cisco Certified Network Associate), MCSE (Windows Server 2008), Cybercrime, Cyber Security, Networking. He is a young professional having exceptional technical and analytical skills, with over 3 years' experience of Computer System/ Network Administration, Information System Support & Security, Network and Server support. He has worked with Techno-ed Pvt Ltd Islamabad, Money Link Exchange Peshawar, and Waseela-e-Taleem - Benazir Income Support Programme. He is currently working as Lecturer with Frontier Comprehensive School & College (FCS), Shergarh, Pakistan.

His research area includes Cloud Computing, Cyber Security, and Cryptography.

Abdul Salam Shah, is currently doing specialization in Management Information System (MIS) from Virtual University of Pakistan. He has completed MS degree in Computer Science from SZABIST, Islamabad, Pakistan in 2016. He did his BS degree in Computer Science from Isra University Hyderabad, Sindh Pakistan in 2012. In addition to his degree, he has completed short courses and diploma certificates in Databases, Machine Learning, Artificial Intelligence, Cybercrime, Cybersecurity, Networking, and Software Engineering. He has published articles in various journals of high repute. He is a young professional and he started his career in the Ministry of Planning, Development and Reforms, Islamabad Pakistan. His research area includes Machine Learning, Artificial Intelligence, Digital Image Processing and Data Mining.

Mr. Shah has contributed in a book titled "Research Methodologies; an Islamic perspectives," International Islamic University Malaysia, November, 2015.

Imran Ijaz, is a Ph.D. Scholar in SZABIST Islamabad, Pakistan. His research areas are Cloud Security, PKI and Security services through PKI under cloud infrastructure. Supervised / Implemented a number of National level network projects. He is serving in Fatima Jinnah Women University, Rawalpindi, Pakistan.