Securing user Authentication through Customized X.509 in Cloud Computing

Imran Ijaz, Muhammad Hasan Islam, Maria Kanwal, Tahreem Yaqoob

Abstract: ***Cloud computing, a highly flexible and user friendly technology of the era providing benefits like accessibility, scalability, reliability and cost effeteness but on the other hand many security and privacy issues arises with the rapid increase of users. Weak authentication process is one of the biggest problem towards breach and most of the time it happened when credentials openly travel over the public internet. To overcome this issue many authentication schemes have been made or modified but problem still persists. In our previous scheme which was based on tunneling using PPTP, effectively works in the scenario [1]. This work is the extension of previous scheme with a customized PKI based certificate to enhance security mechanism through encryption up to 2048 bits.***

Index Terms: Cloud Computing, Secure User Authentication, PKI, VPN Server, X.509.

I. INTRODUCTION

Cloud computing is a technology that offers hardware and software as a service remotely over the public network / internet [1]. The key objective of cloud is same as of Grid and Distributed computing to facilitate end users/customers in term of money and services. Another main objective of cloud computing is to increase the performance and efficiency without spending much money. "Flexibility", "Sold on Demand" are the distinct features which make cloud computing superior and user friendly. Other main advantages of cloud includes reliability, accessibility, scalability, easy to setup and cost effectiveness. Storage space, processing power, Apps and networking equipment are the services offered by a Cloud in different packages as per demand. In spite of such attractive services, still there are some security and privacy related issues in cloud which will be elaborated afterward. The deployment model and service models of cloud computing are as follow:

A. Deployment Model

Cloud can be deployed in following ways:

i. Private Cloud

Private cloud the property of an organization installed on/off premises for organizational IT needs, maintained by the IT team of organization. The best example of private cloud is when personal data of someone can be shareable, changeable/modifiable at any time without any restriction [1] Usually this type of infrastructure configured on premises as it is the dedicated resource of organization it is considered the most secure and expensive.

Manuscript Received on July 2014.

Imran Ijaz, ITC, Fatima Jinnah Women University Rawalpindi, SZABIST Islamabad, Pakistan.

Dr. Muhammad Hasan Islam, Rawalpindi, Pakistan.

Maria Kanwal, Computer Sciences Dept., Fatima Jinnah Women University, Rawalpindi, Pakistan.

Tahreem Yaqoob, Computer Sciences Dept., Fatima Jinnah Women University, Rawalpindi, Pakistan.

ii. Public Cloud

Public cloud managed by organization to serve many customers over the public internet remotely [1]. The organization which owns cloud has responsibility to install and configure cloud setup, whereas the customers can only get services as per their organizational IT needs. This type is comparatively less expensive but less secure than private cloud. This security and privacy issues are the major drawbacks of such type due to accessibility from multiple customers. The agreement between customers and service providers are in term of SLAs. Google appEngine, Microsoft SkyDrive storage space, IBM smart cloud are common examples of public cloud.

iii. Hybrid Cloud

Hybrid cloud a combination of private and public cloud. The concept here is to store sensitive data to private cloud where the non-sensitive data on public cloud. this can be best explained with this simple example a cloud service provider organization who managed a private cloud for their own IT needs but hire another cloud for their customers or vice versa to use public cloud for their IT needs and offer cloud service to customers which they managed. This type of service considered more secure than the private cloud [1]. Another possible example is when organization use public cloud for archiving but keep the currently operational data close or in private cloud.

iv. Community Cloud

Community cloud is another type of cloud services. The concept is to manage some same interest of customers in one cloud. The biggest advantage of this type is organizations used economical cloud infrastructure like private cloud but with an added feature of security and privacy [1]. From provider's point of view, the biggest advantage of this type is as of only same interest.

B. Services Models

Service models of cloud are as follow:

i. Infrastructure As A Service (IaaS)

Infrastructure As A Service (IaaS) as the name shows offers complete infrastructure including servers, storage, software even network equipment as per customer need remotely over the public internet [1]. This type of service usually hired an organization that do not have good IT infrastructure or there might be frequently changes in IT equipment or applications. Amazon and AT&T are the state of the art service providers in this category.

ii. Platform As A Service (PaaS)

Platform as a Service (PaaS) offers platform and development applications over

the public internet remotely as services. The main objective with this type of service is organization can truly focus on development issues rather than the platform and its dependency issues [1]. Amazon, Google and Microsoft Azure are the giants in this category.

iii. Software As A Service (SaaS)

Software as a Service (SaaS) as its name only offers the development applications over the public internet remotely [1]. This is the mostly used model and this type of service covers managerial Apps like management information system, content management system etc. The concept of online gaming when a lot of customers globally connected and playing the game is another commonly seen example of SaaS. Top SaaS providers are Salesforce, Oracle and Microsoft 365. In cloud computing security is as vital as for any other information system. When we talk about security the primary focus will be on user data and users identity. From beginning to till date many techniques formed and modified to achieve security some of them called conventional ones using reputed algorithms and others are modern techniques which are usually the combination of conventional with modified methods to enhance the security. User authentication is one of them. The rapid increase of users with different platforms using open source API's are always be the big problem for cloud service providers. Let we assume that the platform is ideal which mean there is no issue due to platform than our full focus will be on user data and user identity. For securing the user data and user identity there should be some authentication system needed and all users validate through that system. In many cases breech occurs either due to the weak authentication mechanism or credentials travel openly in public internet.

C. Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) is used to setup network security services by using hardware, software and policies to create, manage, distribute and revoke certificates. The concept of PKI is based on certificates which are generated and allocated to users against as their private keys. The certificates also known as X.509. Clients and server follows the procedures to maintain the security however if client or server considers security issue they can revoke the certificate and inform other communicating parties.

D. PKI Services

Generally PKI associates with three services which are:

i. Authentication: Assurance that's the claimant party is "who it claims"
ii. Integrity: Assurance the received message of file is not altered.
iii. Confidentiality: Assurance that the one can see the file and message to whom it for.

E. PKI Components

PKI mainly consists of following components:

i. Certificate Authority (CA): Trusted Authority that is responsible to issue and verify the digital certificates
ii. Digital Certificate: Digital certificates are the public keys generated by CA against private keys of requester
iii. Requester: Requester is an entity requesting for a digital certificates
iv. Registration Authority (RA): Authority who verifies the digital certificate before CA issues to the requester.

II. LITERATURE REVIEW

When we talk about the secure systems user authentication plays an important role to make the system secure. For achieving security using user authentication many techniques had been made and modified according to the scenarios some which are simple and compromised, other are more expensive in term of computational power. Some techniques are failed just because of insecure channel and the credentials travel openly in public internet. Strong authentication process means a good optimal technique (which is optimal in computational power and hard to breech) and the secure channel. It is not possible we secure the system by only making the scheme complex and leave the channel open. Some traditional cloud computing scheme like password based and all its variant (hashing and salting), one time password, zero knowledge are used with biometrics, single sign on and 2FA which are considered as modern schemes to achieve the maximum security and for this researchers uses different approaches like using smart card, dedicated hardware devices and multiple channels (secure channel for credentials and public channel for data). According to [2-5] researchers used dedicated devices including smart cards, USBs and STB boxes which contains the key to initiate authentication process. In one way this will multiply the security as after plug in the device the local level authentication performed before the actual authentication process begins. On the other hand it will end on a breech if these devices lost or stolen. According to [5-6] some researchers used multiple channels a secure channel i-e GSM channel and a public channel i-e a public internet. This approach categorized in 2FA. First level authentication uses public channel after the successful completion of first level the process moves for second level and use the secure GSM channel. Usually the techniques categorized in 2FA used onetime password for second level authentication. The main advantage of this technique is to split the process in multiple steps for if even one part is compromise still the data remain safe. On the other hand the problem of managing another channel and assuming about its security is still big question mark. According to [4] and [7] some researchers believe that more complex scheme will never breech and somehow they are right more complex scheme always hard to breech whether the computations perform at cloud end or client end. But problem is if the scheme is more complex it surely requires a lot of computational power, more bandwidth for more messages during computations. Although we have more computational power and bandwidth these days but still it is not a wise decision to make system busy in computations rather than to perform the job what it is installed for and waste more bandwidth on calculation messages rather than actual data travel.

According to [7-10] some researchers consider Single Sign on, Deffie Hellman based techniques and 2FA work good for achieving security. Somehow they are right all these techniques strengthen the process in some way but on the other hand there are some problems too. For example Single Sign On the good point is covers the human nature of same password for multiple IDs and facilitates the end users to just login and get access to all Apps what if the system breeched on first sign on. Deffie Hellman based technique is also quite impressive both cloud server and clit have their own secrets which they calculate to communicated each other. The positive point of this technique is not much calculation as cloud server and client calculate their own secrets but still there are some problems in this technique like initially both cloud server and client need to transfer messages on the basis of which they can calculate their own keys, secondly what about man in the middle (MTM) attack. Techniques like 2FA seems good as have multiple authentication levels but as authentication levels increase the cost in term of computational power and bandwidth will automatically increase too. Like if 2FA if used secure channel as second factor dependencies of second channel involves and if used other schemes as second factor like zero knowledge, biometrics etc. than need to pay overhead in term of computational power and bandwidth.

III. PROBLEM STATEMENT

Cloud setups are attractive targets for attackers due to their continuous availability on internet and offering different types of services like secure data stored on cloud. For user authentication, there is a need to continuously improve authentication process to avoid unauthorized access on cloud resources. Simple login/passwords provide single layer of abstraction that can be leaked or captured by using key logging or data capturing techniques. To provide more abstraction, different techniques have been suggested. This paper will focus on implementing PKI architecture by cloud providers to issue customized certificates to each user that will be used to establish secure VPN connection thus providing three layers of abstraction.

IV. TRADITIONAL APPROACH IN CLOUD COMPUTING

To build cloud infrastructure, virtual machines are created on high end servers. After that, these virtual machines are configured to host services which are accessed by users like web server, ftp server, email server or data storage server etc. For authentication of users, different mechanism have been adopted like Kerberos, salting technique, Operating system based users or others methods from cloud to cloud service providers.

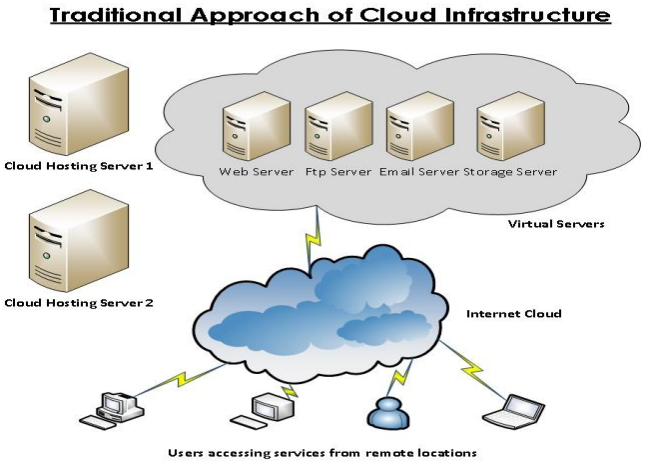

Fig 1. Conventional Cloud Model

In traditional approach, users are asked to enter login and password that is already provided to them. The major issue in this authentication technique is that logins / passwords can be hijacked or sniffed through different methods thus accessing the services by unauthorized users. One of the advantage of this technique is that users have the facility to directly access the services by using live IPs. On the other hand this direct accesses strategy has following issues:

- Exposing Live IPs
- Exposing Addresses (Source and Destination)
- In some cases Exposing Login IDs and passwords (most in hashed form) too.

Open credentials are always the catchy thing for intruders even script kiddies love to play with open credentials although they don't have any mean. Here in this system when addresses are already exposed many chances for traffic bombing which causes the delays and Denial of service (DOS) for legitimate clients, clearly a compromise on performance. Another drawback of this system is there is no control for the internal legitimate client once some employee granted for access he/she can get a full access which will be biggest internal risk.

V. PROPOSED MODEL

According to [12] we already have presented a model to overcome the issue that appears in traditional approach of cloud. This model is the extension of our previous model to strengthen the authentication process. The idea is to build a private PKI setup by a cloud service provider to issue the certificates to cloud users. We can add a dedicated VPN server as gateway of cloud infrastructure. Every user have to use VPN connection and will use his certificate provided to him by the cloud provider. The provided certificate can be customized by the cloud provider in terms of encryption algorithm like DES, AES, RSA etc. or length of the key like 512, 1024 or 2048 bits. Only authorized users having valid certificate will be able to get connected and can access the services. Certificate revocation, validity time of certificate and certificate for each service will be managed by the cloud

provider to maintain security. This model is highly suitable for the organizations that cannot afford unauthorized access on their services or data. This model was implemented and tested to analyze the protection from unauthorized users.

VI. IMPLEMENTATION / TESTING

In our implementation, a cloud was configured using Vmware Esxi and Vcloud Director. PKI was configured on some virtual machines to generate VPN User Certificates. After generating certificates, certificates were distributed to authorized users. Web, Ftp and Data Sharing Servers were created on virtual machines to host services under IaaS. VPN Server was configured and installed at the gateway of the cloud. Users from different locations created VPN Connection, installed provided certificate and successfully connected with the VPN Gateway Server. Connected users accessed the required services and data smoothly. Unauthorized users could not connect with gateway and no access to data or services. This model provides additional security in addition to user credentials.

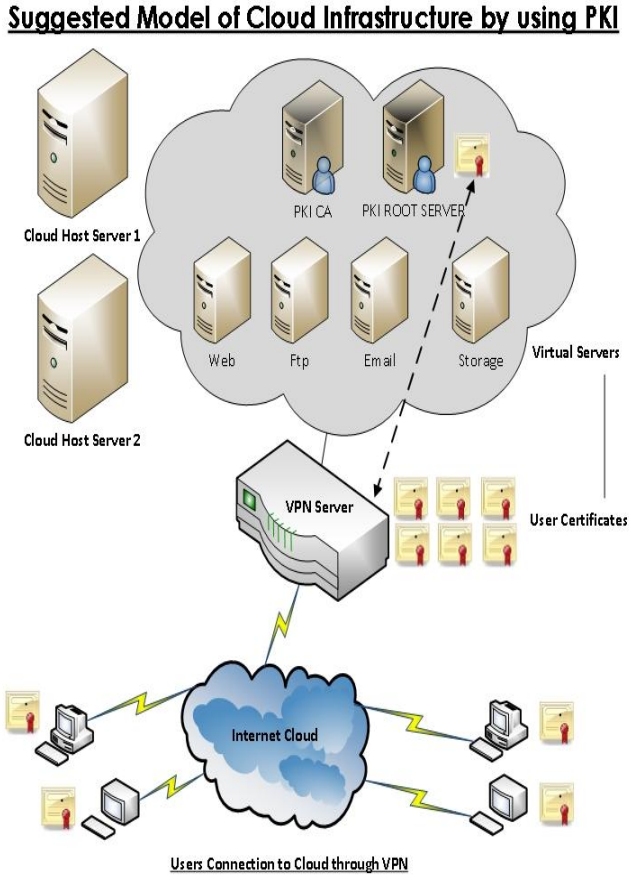

Fig 2. Suggested Model

Response time of services hosted on virtual servers under cloud was measured in both techniques i.e. through direct access and by using VPN connection.

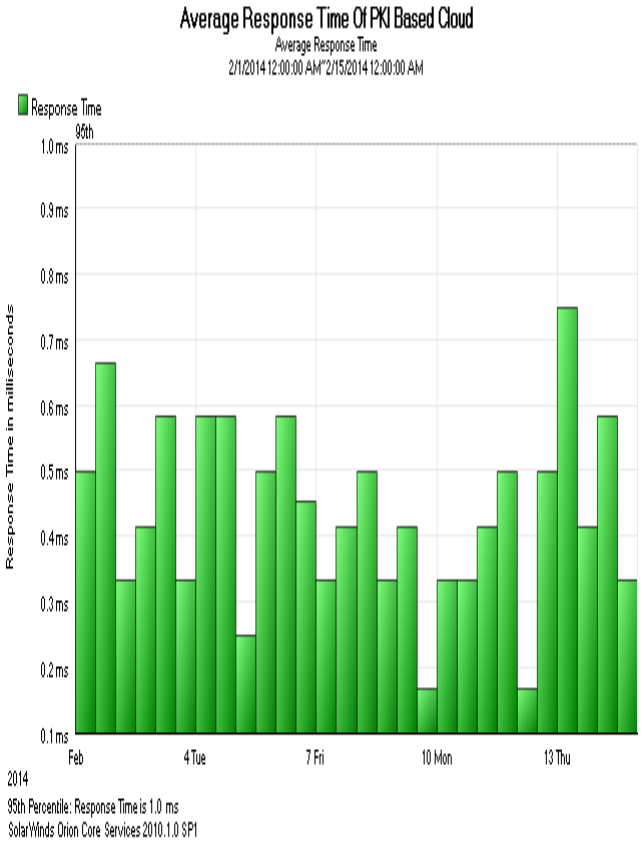

Fig 3. Average Response Time from Servers in Model

Average response time in both techniques was 1ms indicating that by using suggested technique, no significant delay in accessibility of services.

VII. CONCLUSION

Cloud computing the technology of future but facing serious threats in terms of unauthorized access. From beginning to till date many authentication schemes were made and modified to overcome the weak authentication issues and breeches due to weak authentication but most of the techniques have side effects. If we go for the complexity in authentication technique, we have to pay in term of computational power and bandwidth. If we consider multiple channels then the issues is degradation in performance.

Our proposed model provides multi-level security to protect cloud services from unauthorized access. First is uses customize certificate issued by private PKI of cloud service provider, and secondly user have to specify its credentials to connect to VPN Gateway Server to access services. Using right certificate and right user credentials will allow the user to access resources. In addition after successful connection, data transmitted will be through VPN tunnel thus minimizing the risk of data interpretation and unauthorized access from resources.

VIII. FUTURE WORK

The suggested model provides end to end tunnel through VPN connection thus minimizing the hazards of unauthorized access on data or resources.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

The suggested model can be used to authenticate users against different services through type of X.509 certificate issued to users. It will ensure that users will be restricted to access their particular service only. Future work involves testing of such technique against different services.

REFERENCES

1. J. Yang and Z. Chen, "Cloud Computing Research and Security Issues," presented at the Computational Intelligence and Software Engineering (CISE), 2010 International Conference, Wuhan, 2010.
2. T. Chen, H.Yeh, and W.Shih, "An Advanced ECC Dynamic ID-Based Remote Mutual Authentication Scheme for Cloud Computing," presented at the Multimedia and Ubiquitous Engineering (MUE), 2011 5th FTRA International Conference, Loutraki, 2011
3. J. W. Yang, S. H. Kim, J. H. Kim, J. W. Choi, and C. H. Seo, "A Personalized Service Authentication System in Storage Cloud Computing Based D-CATV," presented at the Information Science and Service Science (NISS), 2011 5th International Conference on New Trends, Macao, 2011.
4. Z. Shen and Q. Tong, "The Security of Cloud Computing System enabled by Trusted Computing Technology," presented at the Signal Processing Systems (ICSPS), 2010 2nd International Conference, Dalian, 2010.
5. A. J. Choudhury, P. Kumar, M. Sain, H. Lim, and H. Jae-Lee, "A Strong User Authentication Framework for Cloud Computing," presented at the Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific, Jeju Island, 2011.
6. S.Shanmugapriya, J. G. Begam, M. Anitha, and C. Napoleon, "Two Factor Authentication on Cloud," Journal of Computer Applications, vol. 5, 10 February 2012.[1] J. Yang and Z. Chen, "Cloud Computing Research and Security Issues," presented at the Computational Intelligence and Software Engineering (CISE), 2010 International Conference, Wuhan, 2010.
7. A. A.Yassin, H. Jin, A. Ibrahim, W. Qiang, and D. Zou, "A Practical Privacy-preserving Password Authentication Scheme for Cloud Computing," presented at the Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW), 2012 IEEE 26th International, Shanghai, 2012.
8. A. G. Revar and M. D. Bhavsar, "Securing User Authentication using Single Sign On in Cloud Computing," presented at the Engineering (NUiCONE), 2011 Nirma University International Conference, Ahmedabad, Gujarat, 2011.
9. Imran Ijaz, "Design and Implementation of PKI (For Multi Domain Environment)," International Journal of Computer Theory and Engineering vol. 4, no. 4, pp. 505-509, 2012.
10. Z. Zhang, J. Li, J. Xue-Feng, and Z. Zhang "An Identity-Based Authentication Scheme In Cloud Computing," presented at the Industrial Control and Electronics Engineering (ICICEE), 2012 International Conference, 2012.
11. Z. Zhi-hua, L. Jian-jun, J. Wei, Z. Yong, and G. Bei, "An New Anonymous Authentication Scheme for Cloud Computing," presented at the Computer Science & Education (ICCSE), 2012 7th International Conference, Melbourne, VIC, 2012.
12. Z. Javaid and I. Ijaz, "Secure user authentication in cloud computing " in Information & Communication Technologies (ICICT), 2013 5th International Conference, Karachi Pakistan, 2013, pp. 1 – 5.

AUTHORS PROFILE

Mr. 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. He supervised and implemented a number of National level network projects. He is the author of many research papers published in international conferences and journals. He is serving as Deputy Director ITC in Fatima Jinnah Women University, Rawalpindi, Pakistan.

Dr. Muhammad Hasan Islam, is a Faculty Member at CASE. He has a Vast Teaching and Industry Experience. His areas of expertise are Network Security, Wireless Design and Implementation of Security Policies. Dr. Hasan is the author of a number of research papers published both Locally and Internationally Acclaimed Conferences/Journals.

Maria Kanwal, is from Department of Computer Sciences in Fatima Jinnah Women University. Her research area is Certificate Management

Tahreem Yaqoob, is from Department of Computer Sciences in Fatima Jinnah Women University. Her research area is Security Management under Virtual Private Connection. Certificate Management for Cloud Services.