IJETM

ISSN: 2394-6881

International Journal of Engineering Technology and Management (IJETM)
Available Online at www.ijetm.org
Volume 2, Issue 2, March-April 2015, Page No. 153-162

Implementation of Self-Signed X509 for Cloud Hosted Services

Muhammad Ali*, Imran Ijaz**

Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Islamabad, Pakistan,

*m_alipk2010@hotmail.com, **imran-ijaz@live.com

ABSTRACT

Over the recent years of research in Cloud Computing, different approaches are adopted for securing hosts of Cloud. These approaches give successful results in identifying the authentic request. Sensitive organizations communicate with each other through legitimate request. For establishing a security and privacy a PKI based authentication model is needed. This paper signifies the new approach in implementing a Cloud Based PKI Authentication inside the existing infrastructure of Sensitive organizations. As security is the prime concern for every organization and the requirement to implement it varies from organization to organization, therefore each and every organization embrace their own policies to implement it. The problem of understanding each other security policies is a big barrier and challenging for existing IT infrastructure for implementation purposes. Different techniques and approaches have been suggested so far but couldn't cater the result. Requirement to Secure Cloud host machines Authentication is made possible through this PKI based model which ensures all 5 security services. This PKI model is a multi-domain atmosphere between organization and their data centers for the facilitation and resource provisioning inside the cloud platform. In this model, a Certification Authority (CA) is implemented in the Cloud infrastructure and all users will communicated through this mechanism having different authentication approaches for legitimate access.This article not only presents an architecture but also the implementation of PKI model in multi domain to facilitate data and resource sharing in a secure way.

Key Words: Public key infrastructure (PKI), certification authority (CA), X.509, certificate services.

INTRODUCTION:

The beginning of cloud starts in1969s when ARPANET developed for research Purposes. The idea to interrelate everybody at globe right through getting access to programs and data from anywhere, anyplace, explained Margaret Lewis, director at AMD. It is a basic theme that sounds a lot like, so what we are calling it cloud computing[2]. The scientist John McCarthy who planned the new thought that computation being provided as a public value and since 1960s, cloud computing has developed with lot of varieties, with Web 2.0 being the most current development [1].

Cloud computing, as a new computation paradigm, has been developed and deployed rapidly in recent years. This new approach is built on top of existing Internet technologies and is delivered as service utility. It is the next generation in computation and continuously growing & emerging. It is rapidly becoming one of the most popular and trendytechnology. Cloud Computing means to bring both the applications and services over the cloud and then access these services through browser by high-speed internet as and then pay cloud provider according to usage of these services. Cloud service has three unique features that differentiate it from traditional hosting.

1. Cloud provider sell these services on demand, and organization in return pay for these services.
2. Cloud computing is very Flexible solution, a user can use services according to his need at any given time.
3. All services are managed by cloud provider and user only needs a pc with internet access.

Although cloud computing offers many attractive features but still lack of trust is one of the major issue for customers. Weak authentication schemes cause many loop holes which invite intruders to breach the customer data. The scope of this study will focus on authentication behavior of customers and strengthen the user authentication schemes. As Cloud computing is swiftly evolving as a new prototype for delivering services of computing as a utility. Cloud computing is relatively similar to grid computing, in which different hardware resources are shared to attain a common objective.

The Internet has become a main stream for all sort of communication framework and is also vulnerable for all known & unknown attacks. These attacks comprises

number of network threats like wiretapping, industrial espionage, Man In the Middle attacks and fabrication of sensitive data etc. So as to repress these dangers, Security Services like secrecy, respectability, verification, and non-denial are least necessities for anticipation. Association have executed a few measures to thwart their region. These necessities are upheld by various security arrangements. One of them is a Public Key Infrastructure (PKI). Most of the protocols for secure communications like email, web service, ftp, SharePoint, virtual private networks, and authentication systems use PKI.In this paper we will critically review Cloud Authentication through PKI in existing infrastructure of sensitive organization. We will also see the options available to us, how to increase the utilization of Applications / Hardware & Storage resources in cloud environment and how to establish a trust relationship in our virtualized environment to achieve the optimum results.

A. Cloud Deployment Models

There are four commonly used cloud deployment modelsgiven as [4].

i. Public Cloudis a model of computing providing services to community for pay per usage. It includes several stake holders ranging from government organizations to services industries.

ii. PrivateCloudis a model owned, operated and managed by a single organization or an enterprise for its employees.

iii. HybridCloud is a model consisting of two or more entities having distinct infrastructure (i.e., either public, private or community cloud) to share their resources and provide services to the community.

iv. Community Cloud is a model in which groups or specific organizations share their cloud infrastructure exclusively used by them. Mainly worked, operated, managed and owned by academia or third party.

B. Cloud Service Models

i. Infrastructure as a Service (IaaS**)**:

The IaaS modelconsists of servers, storage appliances, network resources and other telecommunication equipment's capable of deployment and providing services in Data Center like environment. This model bring benefits to users for acquiring services as mentioned above for rental basis and reduce their costs of purchasing hardware/software etc. Google App Engine [18] and AMAZOM Elastic Compute Cloud (EC2) are the industry leading vendors providing IaaS like services to community [20].

ii. Platform as a Service (PaaS):

It is a software prototype model independent of existing Operating Systems. Users can develop their customized applications and deploy on their hosted server. Secondly this model is primarily used for accessing Web Services, SOAP and other subscriber choice provided to provision these services. It also reduces the cost and difficulty of software buying, retaining and deployment. The Amazon Simple Storage Service (S3) is an example of PaaS.

iii. Software as a Service (SaaS):

The SaaS model comprises different softwares / applications for the on-demand usage. Users are provided different services for their choice to adopt and deploy accordingly to their requirement. The SaaS model is independent of location and transparent to user for accessing their service. Benefits of this model are the cost reduction of purchasing software along with licensing issues, operational and maintenance. TheGoogle App Engine, salesforce.com,Facebook.com andMicrosoft's Azureare examples ofSaaS [19].In other words, the cloud computing is an assortment of PaaS, SaaS and IaaS. The employees working in an organization can be users or providers of cloud computing services in accordance with the organizational scope and the control over the IT environment Chen [17].

I. CHARACTERISTICS OF CLOUD COMPUTING

There are some key features of cloud computing given:

A. Virtualization

Virtualization technology provides an interface between various elements either from the software point of view or from the hardware. Software virtualization consists of applications, programs, services like providing an API to facilitate users from connecting their network to other locations of the web and seamlessly experience as it is in their vicinity. Software virtualization also provides flexibility to provision those resources which are not available to us in our hosted cloud environment. Techniques like Storage as a Service (STaaS) is adopted on the main vendors of the World for its magnificent integration of real storage atmosphere.

B. Agility

Agility refer to the term in which how optimized our infrastructure to provides resources on time and have 99.99999% down time. Through agility and robustness every organization can achieve its desired goals and will stay in the market for decades. Consequently it is also adopted over application point of view and other area of expertise to give better results through efficient and effective way.

C. Application programming interface (API)

APIs are used on software level to retain smoothness of

application behavior and maintaining its integrity with other RPC (Remote Procedures Calls) through built-in subroutines and functions. Different functions on calling interact with its APIs to perform certain jobs. Jobs can be to take print from the network printer and talk to print spooler if another jobs is in queue. On the cloud spterm there are many APIs which are used to create, manage and hold the resources over the hosted platforms. Mainly built and executed on the Platform as a Service (PaaS) and Software as a Service (SaaS). Examples are RESTful (Representational State Transfer), SOAP (Simple Object Access Protocol), AWS (AMAZON Web Services) etc. based APIs used to attain and perform its tasks.

D. Cost

Cost is the major factor in developing any type of IT setup. It depends on the number of employees a company has and the type of business in which the company owner wants to excel. Similarly in the business of cloud computing, cost factor is minimized due to several reasons. One factor is that now all IT resources are on the Internet and usually users don't have to purchased new IT equipment's ranging from few servers to a big Data Centers. This facility not only reduce their hardware cost for consuming such type of resources and also eliminating other expenditures like the amount given to the technical and non-technical staff for their salaries .

Second most prominent factor is the reduction of electric power consumption, as company will maintain cool solutions to its Data Centers and will have to install a huge plant for running all servers by 24/7/365 days. Energy crises are the big hurdle to bear for any business concerned personnel. Their Data Centers will consume not only huge amount of electric power but also acquired a backup plan for installing a Battery backup unit for up time and in this way all factors lead to a huge investment on their own level is required to maintain and run all their company services. Similarly a cloud solution provide not to purchase extra hardware or build a Data Center but to acquire any type of service on pay as you go method. It depends on which type of cloud model we acquire to attain services over it and adopting the paying method over it.

E. Location independence

In the cloud computing models the location of any user is transparent as users are provided ID and login password to connect their cloud over cross platform environment. Users are able not only to connect with their Desktop PCs but a provision of other devices like connection through Mobile/Smart Phones and any type of wireless medium easily and safely. Hundreds of Data Centers location in various part of the World are providing these services over heterogeneous and homogeneous platform to make sure that nobody can have any sort of problem during login and availing all the services over the cloud.

F. Reliability

Reliability is a factor on every forum it enhances the trust and establishes bond between two different entities (organizations, corporations, governments or even two different countries). Consequently on the cloud computing platform a reliable resource can extend the life and performance of the cloud services. Reliability between APIs and its association with other functions enhances the portability of cloud services over un-trusted networks. Reliability play a more special role with redundant links in case of failure occurs and possess the better management to business contingency plans and disaster recovery mechanisms.

G. Scalability

Scalability is the assurance for the service provider for the performance measuring principles and gives best results if it is overloaded. Scalability is measured in terms of fine grained, optimized, isolated, error free and robust architecture for the implementation of any type of service over it. The benchmarks of scalability are the maximum points / thresholds for measuring capacity and ensuring optimum results with limited and non-viable resources.

H. Security Services

Security provides the main pillars to any organization:. No matter which type of organization is holding what type of data, it is the prime responsibility to secure its assets. Similarly in the case of cloud computing, security can be generalized into various portions starting from user identity to massive data processing storage device integrity. Security can be applied on the operating system (OS) level, its file system, ports, I/O device management and User access with accounting. Similarly on the cloud computing it is applicable on the applications credentials i.e., user id and password. Security can be applied on the services like Web Services, Access Protocols, and RESTful APIs etc. to ensure that the applications are providing legitimate access with this service integration.

On the network level, there are various mechanisms to be implemented in order to execute our cloud services over the insecure channel like installing firewalls both in the shape of software and hardware based to monitor proactively for any malicious activity over the networks and also inside the network as well. Several encryption algorithms are developed to secure our transactions and provide an approach to surf the cloud environment without fear. Security also gives us the privacy of our identities

Over the cloud hosted services. Hence it will be hard to say that without security we can achieve every milestone over the cloud environment.

There are eight elements identified by National Institute of Standards and Technology (NIST): governance, compliance, trust, architecture and software isolation, identity and access management, availability, incident response, and data protection Mell and Grance [19].

II. LITERATURE REVIEW

The essential inspiration for embracing cloud is its minimal effort; on the other hand, on the other side, endeavor gets to be capable and responsible for general security of the outsourced administrations by Jansen [7]. The key security issues correlated to distributed computing are sorted out into a few classes, for example, information assurance, trust, character administration, structural engineering, programming segregation and accessibility. The association must consider the potential security dangers before embracing the cloud. The security of cloud framework generally relies on upon trusted registering and cryptography.

The business or venture information must be secured with proper and dependable approaches or methodology whether in the undertaking's own particular datacenter or in the cloud environment. It gives a beginning stage with a rundown of basic outsourcing necessities like Security and Privacy Standards, Compliance and Regulatory Issues, Service Level Agreements (SLAs), Certificates and so on. Also, the danger administration is likewise fundamental for the business endeavors before movement to cloud. The danger must be precisely moderated on the grounds that the association is responsible for its asset security

The review, SLAs, accreditations and danger treatment techniques being a vital structural lump of cloud security and controls are characterized into a solitary system examined in by Julisch and Hall [8]. An Information Security Management System (ISMS) comprises of strategies, techniques and components that a venture uses to build, actualize, work, screen and enhance the data security. The skeleton alluded to virtual ISMS is contrasted and the traditional ISMS for those associations where IT administrations are to some degree outsourced. The virtual ISMS is really an organized approach to oversee hazard and hierarchical resources over the cloud. In addition, as cloud customer and supplier are together in charge of information security and control in the cloud, so they must receive virtual ISMS as a standard grumbling administration process for the assurance of imparted resources. In this manner, it is more essential from customers prospective that they must think about what they are buying with cloud.

Mohammad [9] highlighted the noteworthy key drivers and imperatives for secure distributed computing from a societal and mechanical prospective. The distributed computing is a rising time of processing which is confronting numerous difficulties of information insurance and wellbeing. The trust, protection and client approach towards distributed computing are the social issues while on the other side encryption, versatility and unwavering quality, information rights and straightforwardness are the genuine innovative issues in distributed computing. As per the creator, the most cloud clients are unconscious of the danger of putting away and transmitting private data in an imparted environment. Hence, scratch mechanical demands like consistence, straightforwardness, encryption, respectability and multi-tenure ought to be tended to painstakingly. The straightforwardness is the greatest test for the undertakings at present, and because of which they are hesitant to change to distributed computing environment. When the cloud gets to be straightforward and the clients have full control to get to, oversee and cover the condition of information and administrations, at exactly that point it will help expand the trust and minimize the social and innovative stipulations.

The innate issues of information security, administration and administration regarding control in the distributed computing are examined by Mehmood [10]. The real issues in cloud information security are: information protection, information insurance, information accessibility, information area and secure transmission. The issue of putting away information over the Trans boarder servers is a genuine concern of customers in that capacity sellers are administered by the neighborhood laws and, thusly, the cloud customers ought to be conscious of those laws. The information accessibility is additionally an essential concern and administration downtime must be as per the predefined SLAs. In addition, the cloud supplier ought to guarantee the information security including information privacy and respectability. The cloud supplier must impart all such concerns to the customer and manufacture trust relationship in this association. The cloud seller ought to give assurances of information security and certain locale of nearby laws. The principle center of the paper is on those information issues and difficulties which are connected with information stockpiling area and its movement, expense, accessibility and security.

The protection danger connected with distributed computing has brought up genuine issues by Svantesson and Clarke [11]. Accordingly, the cloud suppliers ought to put set up clear and straightforward methods and arrangements concerning legitimate structure keeping in mind the end goal to addition clients trust. Also in the meantime, the clients should likewise assess precisely the information security and protection issues before going into the coliseum of distributed computing. Moreover, the lawful purview issues identified with information in local and trans-outskirt mists ought to likewise be considered. These issues must be tended to and arranged with common seeing in fitting way. At the point when numerous clients utilize the cover over trans-outskirt, it builds the legitimate ward load and the obligation of cloud supplier. In this setting, the customer's hazard and rights need to be tended to and saw in point of interest. In addition, it is vital for customers to know the cloud supplier's neighborhood laws identified with information protection and assurance. The cloud supplier needs to create and make information insurance systems, arrangements and laws and afterward make mindfulness about such laws among the clients. The expense viability is one of the significant inspirations for the associations ready to change to the distributed computing independent of the in all cases security examination of the cloud supplier.

The Identity and Access Management (IAM) conventions and norms are the paramount information security angles talked about in by Almulla and Yeun [12]. The IAM is a sufficient level of security for authoritative resources through executing fitting strategies. The rising IAM difficulties can be minimized through examining validation, approval and reviewing issues. The IAM lifecycle comprise on five stages: Provisioning and DE provisioning, Authentication and Authorization, Self-Service, Password Management, Compliance and Audit.
Besides, diverse guidelines and conventions like Security Assertion Markup Language (SAML) and Open Authentication (Oauth) convention are utilized to manage characters in the cloud. To this end, the associations must get ready IAM method, structure and comprehend the IAM lifecycle before movement to cloud. The IAM ought to likewise be legitimately executed to guarantee the common verification, examining and approval for distributed computing administration.

The distributed computing is turning into a prominent and appealing ideal model with bunches of profits, then again, there are some particular inquiries identifying with its capacity to backing scientific examination by Relly et al. [13]. The creator has mostly examined the cloud qualities, models, and building design. The measurable examination has its roots for information recuperation and, discovering, advanced confirmation from law requirement viewpoint. In distributed computing the scientific status is not completely considered by the majority of the associations, so there is have to return to or create new systems to meet the current cloud prerequisites. Additionally, the criminological examination has advantages and disadvantages which need to comprehend amid measurable preparation. Additionally, the scientific examination finding in virtual machines (Vms) has blended methodology of favorable circumstances and impediments. Hence, the scientific agents group is obliged to create new techniques and strategies to conquer the distributed computing legal investigation challenges.

The informationclassified, validation and access control issues in distributed computing have been tended to by proposing a structure to expand the cloud dependability and reliability by Patil et al. [14]. A framework to uses cryptographic calculation Diffie-Hellman for secure correspondence as opposed to key appropriation administration is proposed in (RSA, 2008). Such a framework ordinarily comprises of three modules: Administration Module, Authentication Module and Encryption Module. Every module has diverse however interconnected capacities. The organization module is utilized by the cloud supplier for client enrollment and organization. While the verification module is utilized for confirmation of clients and encryption module utilized for information encryption. The validation acknowledgment is a two way transform. Firstly, the framework requires the client to enter typical login and watchword and after that it produces one time secret key and sends on the client portable for verification. Once the one time secret word is supplied, the framework verifies the client and gives the framework access. The proposed framework was tried on Java Remote Method Invocation (RMI) in cloud environment (Oracle, 2007). The framework kills the cloud over-burden and keeps it from man in the center assault.

Mirashe et al. [15] examined the distributed computing administration and organization models with illustrations and its points of interest in subtle element. The creator further characterizes the classes of cloud clients e.g. families, group and companies. As indicated by the creator, information security is the significant issue in distributed computing. The client's information could confront genuine dangers in the event that it is decoded in plate or memory or over the system in the cloud. The second real concern is identified with evaluating of open

cloud. The cloud suppliers are regularly hesitant to do reviewing for their assets and base. The to wrap things up issue is legitimate ward over the cloud. The undertakings must consider these issues before receiving distributed computing.

Sun et al. [16] highlight the key security, protection and trust issues in existing environment of distributed computing and help clients to perceive the substantial and immaterial dangers connected with its utilization. As indicated by creators, there are three noteworthy potential dangers in distributed computing, to be specific, the security, protection and trust. Security has the fundamental part in present period of since a long time ago imagined vision of registering as utility. It can be separated into four sub-classes: security systems, cloud server observing or following, information classified and keeping away from pernicious insiders' illicit operations and administration seizing. Besides, the creators highlight the essentialness of information security in distributed computing. It is a key point from client viewpoint and basic to comprehend its issues like client control over information and legitimate purview prerequisites. Also, the trust is a complex relationship among cloud customer and supplier and it ought to be untimely before receiving cloud. The trust between cloud supplier and customer ought to be measurable and dependable to settle on reliable choice. The trust can be isolated into four sub-classes: trust assessment, trust relationship, trust degree and trust observing.

The security control estimations in distributed computing are equal to the ones in the traditional IT setup by Chen and Zhao [17]. The customer ought to know answers to the seven security questions before making the choice of cloud suppliers. These inquiries are about information area, information isolation, recuperation, favored client access, consistency consistence, scientific backing and feasibility on long haul premise. Besides, the customer needs to only break down the information security, insurance and security issues all through the information life cycle over the cloud. The information life spin passes through seven stages: information era, exchange, utilization, offer, stockpiling, archival and decimation. The information distinguishing proof, information disconnection and protection security are the essential concerns and must be kept into thought amid the configuration and improvement of cloud-based applications. The incorporated and complete security arrangements are relied upon to meet the information security and insurance target top to bottom.

III. COMPONENTS OF PKI

Components of a PKI embrace system components such as one or more Certification Authorities and a certificate repository; documentation including a Certificate Policy document and one or more Certification Practice Statements and trained personnel performing trusted roles to operate and maintain the system.

The main mechanisms of PKI infrastructure are:

1) *Certifying Authorities (CAs)*–This components signifies to ensure that certificates areissued and revoked with digital certificates in PKI domain.

2) Registration Authorities (RAs)–It validates all those requests pending for issuing certificates and identity of each & every end users.

3) Repository –This components is used to store and distribute certificates and revocation of certificates through the process of certificate revocation lists(CRL). A technique which is used to issue all certificates periodically by the CA and are listed in the queue of certificates that are no longer valid.

4) Archives –The basic purpose of archive is to store all information readily available to Certificate Authority and possessing all information to be archived which are easily provided and no modification is recorded when the archive process is going on.

5) End Entity - End entity are those actors for which digitalcertificates are issued.

IV. ARCHITECTURE OF PKI

Architecture& Structural planning of a PKI is made out of operations and security approaches, security administrations and conventions that help interoperability utilizingPublic key encryption and key administration authentications. In PKI an automated declaration issued by CA and requisitions are normally transformed by the Registration Authorities (RA). The obligation of a RA is to dissect singular client who analyzes every provision and advises the CA, which is closer to the level of certainty of the applicant by checking the level of trust, CA issue the endorsement.

A. Stand Alone Root CA

Standalone Root CA is actualized where we require a disconnected from the net Root CA. Remain solitary and is not coordinated with dynamic Directory. However data from the CA, for example, CDP and AIA, could still be distributed to Active Directory. Ordinarily the Stand Alone CA is a part of its own workgroup rather than being a part of a space. It is detached from the system just open to the administrators of the CA server.

B. Enterprise Root CA

Enterprise Root CA is comparatively easy to implement as there is only one server required to establish PKI and there is no subordinate CA servers and certificate chaining. Enterprise CA server is integrated with Active Directory. An Enterprise CA can be used to auto enroll certificates in an Active Directory environment.

C. Stand Alone Issuing CA

A Stand Alone Issuing CA means that the CA server is a subordinate CA server and it has gotten its CA certificate signed by another CA server. Typically this type is used when the CA server won't be issuing certificates to objects in an Active Directory domain, or using an offline policy CA server in three-tier PKI hierarchy.

D. Enterprise Issuing CA

An Enterprise Issuing CA is a part of an Active Directory space and is coordinated to Active Directory. Client and workstation records can enlist or auto enlists for authentications from this CA. The CA server gives the same usefulness as an Enterprise Root CA server, yet the Enterprise Issuing CA is a subordinate CA server.

V. TIERS of PKI

Most PKI setups will have one, a few levels. With one level there is just Root CA which is in charge of issuing and denying all the authentications. In a two level environment there are logged off Root CA and one or more subordinate CA servers. In a three level environment there are a logged off Root CA, one or more subordinate arrangement CAs which can additionally be disconnected from the net. These approaches CAs will administer the arrangement of the subordinate CAs underneath them, the issuing CA servers.

VI. PROBLEM STATEMENT

Cloud setups are appealing focuses for hackers because of their constant accessibility on web and offering distinctive sorts of services like secure information stored on cloud storage. In order to authenticate clients, there is a need to consistently improve authentication process, so that unauthorized user with malicious intention could be stopped from getting access to the resources hosted on cloud.

Simple login/passwords give single layer of abstraction that can be spilled or caught by utilizing key logging or information catching methods. To give more abstraction, distinctive strategies have been recommended. This paper will concentrate on actualizing PKI construction modeling by cloud suppliers to issue customized certificates to each one client that will be utilized to make secure connection

VII. PROPOSEDPKI MODEL FOR INTER-CLOUD DOMAINENVIROMENT

This model is design 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. Every user 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. In our implementation, a cloud was configured using VmwareEsxi and VCloud Director. PKI was configured on some virtual machines to generate 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. Users from different locations were provided certificate. 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.

The prime and focal objective of our PKI model was to facilitate exchange of information securely between host and Cloud domain. List of models with detailed architectures have been designed but we have only selected the most secure and obvious one among rest of all.

In our finalized model, we implement single tier PKI. The single tier PKI consists of three main components. A domain controller, an enterprise Root CA, web server and ftp server. A domain controller will run active directory – integrated DNS and host LDAP CDP and AIA.

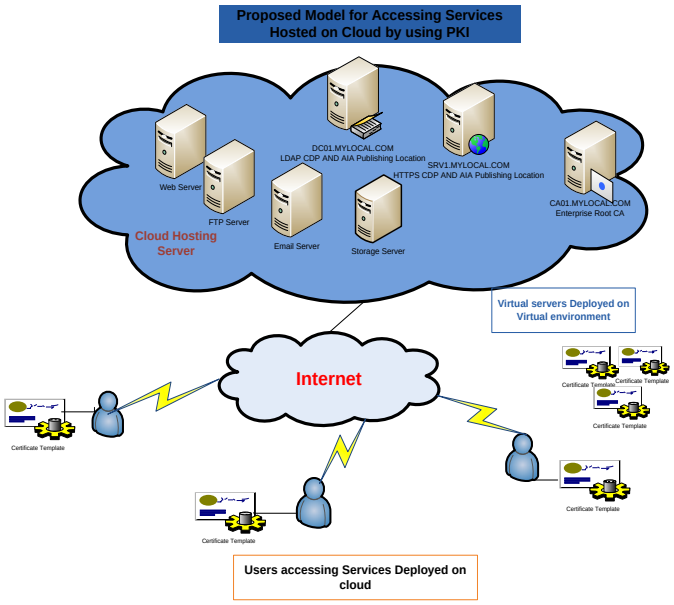

Figure 1: Proposed Model

Internet information services (IIS) web server that will host the HTTP CDP and AIA. A vm machine named "DC01" is installed on VMware cloud. On this DC01 vm an active directory forest was installed and "MYLOCAL.COM" domain was created on this DC01 VM and finally DNS was configured in order to IP to name, and name to IP resolution.

Furthermore new VM was created with name SRV1 and to prepare HTTP web server and CDP for AIA publication. After successful installation of it, a VM with name "CA" was created in VMware cloud. On this CA VM, CApolicy.inf was created was for enterprise ROOT CA. In this CApolicy.inf, URL, renewal key length, renewal validity period and other parameter were defined. After this step Enterprise Root CA was installed on this CA VM. After successful installation of Root CA ,CDP and AIA were configured on it. Finally "MY LOCAL.COM" domain Root CA certificate is published to AIA. Ftp and data storage Vms were configured in VMWARE cloud in order to provide file transfer and data storage services to users.

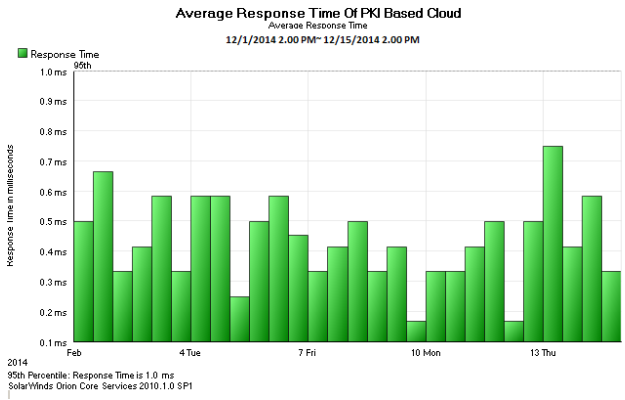

Figure 2: Average Response Time from Servers in Model

In our implementation, a cloud was configured using VmwareEsxi and Vcloud Director. PKI was configured on some virtual machines to generate 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. Users from different locations were provided certificate. 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.

VIII. CERTIFICATE FLOW PROCESS

Whenever computers is connected to respective network

and joined with defined domain, that computer will get the computer certificate. For secure and reliable communication, policy was configured in domain through GPO to issue the certificate to users who only member of respective domain only.

After establishment, design and execution of complete model, the execution of every server was broke down. All procedures were running easily without over loading the servers and real expand in system activity.

The execution of actualized model was broke down on the bases of deferral, reaction time, reachability and way acceptance. Accessibility of CA Server and testament activity were examined to screen the heap and its execution. The results indicate great execution against every assessment.. The results indicate great execution against every assessment.

IX. CONCLUSION

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 Server to access services. Using right certificate and right user credentials will allow the user to access resources.

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. 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.

X. FUTURE WORK

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, so overcome this problem we can add a dedicated VPN server gateway and our future work is to design a model in which every user have to use VPN connection and will use his certificate provided to him by cloud provide

REFERNCES

1. N. Leavitt, "Is Cloud Computing Really Ready for Primetime?"*IEEEComputer*, 2009
2. *L. M. Vaquero1, L. Rodero-Merinolet al, "A Break in the Clouds: Towards a CloudDefinition", Computer Communication Review,Volume 39, no.1, January 2009. Online]. Available: http://ccr.sigcomm.org /online /files/p50- v39n1l-vaqueroA.pdf*
3. Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing" , 2009 http://www.nist.gov /itl/ cloud/upload/cloud- defv15.pdf
4. C .Yanpei, P. Vern, *et al*, "What's New about Cloud Computing Security?,"Electrical Engineering and Computer Sciences .University of California, Berkeley. Technical Report No. UCB/EECS-2010-5, January 20, 2010
5. M. Willis, "Cloud Computing and the Enterprise", *IT Management and Cloud,* 13,February,2008. [Online] Available: www.johnmwillis.com/ibm/cloud-compu - ting -and-the- enterprise,
6. W. Iqbal,M. Dailey, *et al,* "SLA-driven adaptive resource management for web applications on a heterogeneous compute cloud". *In Cloud Computing* , Heidelberg. Berlin:Springer,2009.pp. 243-253
7. W. A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing", 44th Hawaii Inter- national Conference on System Sciences ,IEEE,2011
8. K. Julisch and M. Hall, "Security and Control in the Cloud", *Information Security Journal: A Global Perspective,* vol. 19, pp. 2099-309,2010
9. D.Mohammed, "Security and Cloud Computing: An Analysis of Key Drivers and constraints", *Information Security Journal: A Global Perspective*, vol. 20, pp. 123-127,2011
10. Z. Mehmood, "Data Location and Security Issues in Cloud Computing", International Conference on Emerging Intelligent Data and Web technologies, IEEE, 2011
11. Svantesson and R. Clarke, "Privacy and Consumer Risks in Cloud Computing", *Computer Law and Security Review*, vol. 26, pp. 391-397,2011
12. S. A. Almulla and C. Y. Yeun, "Cloud Computing Security Management".

13. D.Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", 2012 International Conference on Computer Science and Electronics Engineering, IEEE.
14. Google Compute Engine, http://cloud.google.com/products/computeengine.html
15. Google Apps, "Get online email, calendar documents and more working for your organization", http://www.google.com/apps/index1.html.
16. Amazon, "Amazon Elastic Compute Cloud (Amazon EC2)", http://aws.amazon.com/ec2/
17. "A Framework for Data Storage Cloud to Provide Security by Implementing Encryption through User Private Key", International Journal of Emerging Trends in Science and Technology (IJETST), pp.932-938, Vol 1, No 06 (2014), August 2014, ISSN 2348-9480
18. "Securing Cloud Infrastructure through PKI", IEEE International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2014. 11-13 July 2014, pp.1-6.
19. "Securing user Authentication through Customized X.509 in Cloud Computing", International Journal of Soft Computing and Engineering (IJSCE), pp.90-94, Volume-4, Issue-3, July 2014, ISSN: 2231-2307
20. "Design and Implementation of PKI for Multi Domain Environment", International Journal of Computer Theory and

Mr. Muhammad Ali is MS (ISM) from SZABIST, Islamabad Pakistan. He is serving as Assistant Manager in Public sector Organization. His research areas are Cloud Security, PKI and Security services through PKI under Cloud Infrastructure, Cyber Security, Pen Testing, IT Auditing.

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. Supervised / Implemented a number of National level network projects. He is serving in Fatima Jinnah Women University, Rawalpindi, Pakistan.