www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 4 April 2015, Page No. 11257-11266

Authentication at Single-Point-of-Access in Cloud Environments

Rizwan Ahmed*, Mr. Imran Ijaz**

*Shaheed Zulfiqar Ali Bhutto Institute of Science and Technology, Islamabad, Pakistan

**FJWU Rawalpindi, SZABIST Islamabad, Pakistan

*Rizwanahmed936@hotmail.com , **imran-ijaz@live.com

***Abstract* - Cloud computing is a rising innovation and increase consideration in scholastic and business range. Assets are pooled and offer with clients on interest. With a specific end goal to give better execution of cloud environment, undertaking planning is a paramount issue. The objective of the study to explore the different environments of the cloud infrastructure w.r.t security. It is big challenge for the cloud service provider company to implement the security and meeting the highest level of the service with the providing quality service and secure environments to the clients. This is how the Cloud service providing companies build the trust relationship with their clients. The propose model is the security optimization of the already implemented security in the cloud environments along with the quality service in terms of required bandwidth and required infrastructure like Saas, Paas, or Iaas. Meeting both, quality of service and security, Cloud service Provider Company has to do lot of working as the cloud has multiple integrated infrastructures. It will be a big loop hole if a cloud service provider company give access to their actual servers or live IPs to provide services to the clients. There will be lost of resources, time and availability of resources to the legitimate users. The primary objective of the study is to build a model which provides us un-authenticated and un-authorized users blocked from one single point which is other than the service provider to the clients of Saas, Paas, or Iaas and the resources to authenticate and authorize a user with in the cloud are used by the legitimate users.**

Key words: - ***Cloud Computing, Authentication, Single-Point-of-Access***

1. INTRODUCTION

Cloud computing has been considered as one of the swearing up and down to solutions to our expanding interest for getting to and utilizing assets provisioned over the Internet. It offers compelling handling and stockpiling assets as on-interest administrations with lessen cost, and build effectiveness and execution. Nonetheless, with these guaranteeing offices and profits, there are still various specialized boundaries thwart using the cloud, for example, security and nature of administrations. The servers and the network have the basic requirements to establish a cloud infrastructure. So as the cloud is also part of a huge network which is internet and internet has lot of malicious things involved. So we have to keep our servers and network away from those type of attacks in which the servers and network are directly exposed. This archive addresses regular servers that utilize general working frameworks (OS, for example, UNIX, Linux, and Windows. The focus of this research is to investigate potential security issues identified with securing cloud computing specifically related to the servers and the IP addresses in the practice environment. The model shows a practice approach with the help of common technologies that cloud environment must be secure and not for everybody as the resources are valuable to use.

1.1 Cloud computing in today's World of Huge Computing Environments

To clarify the vitality of distributed computing will be simpler in the event that we consider this illustration how about we say's the obligation of some IT official of substantial corporate is to verify more representatives have the right hard and programming according to their improvement necessity. One choice is to purchase all equipment and programming needs and oversee authorizing issues of running programming and continue expanding fittings as with new contract. Then again the alternative is to load one application. That application would permit specialists to log into a Web-based administration which has all the projects the client would requirement for his or her employment. Remote machines claimed by an alternate organization would run everything from email to word transforming to complex information investigation programs.

Cloud Computing gives Infrastructure-as-a-service (IaaS), Platform-as-a-service (PaaS) and Software –as-a-Service (SaaS) depending on the requirements of the client.

I.2 SECURITY IN CLOUD COMPUTING

There are various dynamics of the cloud computing security at the different levels. Security infrastructure provided reflects the environment infrastructure and the platforms involved in the cloud. Below are the some security common terms involved in different cloud computing environment.

1.2.1*Trust*: -Trust in a cloud environment depends vigorously on the chose organization model, as administration of information and applications is outsourced and designated out of the manager's strict control. In customary architectures, trust was implemented by an effectivesecurity strategy, which tended to stipulations on capacities and stream among them, obligations on access by outer frameworks and enemies including projects and access to information by individuals

1.2.2 *Data Confidentiality*: -Information secrecy in the cloud is related to client verification.Securing a client's record from burglary is an occurrence of a bigger issue of controlling access to protests, including memory, gadgets, programming and so forth. Absence of solid confirmation can lead to unapproved access to clients account on a cloud, prompting a breach in protection.Unapproved access can get to be conceivable through the misuse of an application weakness or absence of solid ID, raising issues of information secrecy and protection. In addition,the cloud supplier is in charge of giving secure cloud occasions, which ought to guarantee clients protection. Protection is the longing of an individual to control the exposure of individual data.

1.2.3 *Data Integrity***:** -Data Integrity is a key part of Information Security is uprightness. Respectability implies that advantages can be adjusted just by approved gatherings Orin approved ways and alludes to information, programming and equipment. Information Integrity refers to securing information from unapproved erasure, alteration or manufacture. Dealing with an element's permission also rights to particular endeavor assets guarantees that significant information and administrations are not misused, abused or stolen. By avoiding unapproved access, associations can accomplish more prominent trust in information and framework respectability.

1.2.4 *DataAvailability*: -Information Availability alludes to the property of a system being accessible moreover usable upon enthusiasm by an endorsed component. Structure openness fuses a systems ability to shoulder on operations really when a couple of forces misbehave. The skeleton must can move ahead with operations even in the probability of a security break.

To reach the destination of highest level of security in cloud computing environments are basically:

• To guarantee the accessibility of data conveyed between the cloud service provider and the customer

• To keep up the honesty of data conveyed between the cloud service provider and the customer

• To give control over access to administrations

• To validate the personality of conveying accomplices (peer substances) and where essential.

While including,

• To guarantee the privacy of data hang on taking interest frameworks.

• Clear detachment of information and courses of action on the virtual level of the cloud, guaranteeing zero information spillage between distinctive applications.

• To keep up the same level of security when including or uprooting assets on the cloud storage.

1.3 AUTHENTICATION AT SINGLE-POINT-OF-ACCESS

Cloud computing is a cutting edge technology in today's world of large computing infrastructures. Its open sending model infers preceding onward premises IT structural planning to outsourced mists oversaw by a cloud supplier. In that capacity, clients will need to trust the suppliers, since they may hold possibly touchy information. In Software-as-a-Service (Saas) mists, validation is restricted to the product they offer, conversely to what happens in Platform-as-a-Service. (Paas) that permits clients conveying what they best see fit. In Infrastructure-as-a-Service (Iaas) mists, Virtual Machines (Vms) may be assembled in virtual server farms and can be gotten to through remote association conventions. Confirmation is discriminating in cloud and particularly for the ready for and frameworks. Cloud computing is an as of late created new innovation for complex frameworks with monstrous scale administrations offering among various clients. In this manner, validation of both clients and administrations is a noteworthy issue for the trust and security of the distributed computing. SSL Authentication Protocol (SAP), once connected in Cloud computing, will get to be complicated to the point that clients will experience a vigorously stacked point both in calculation and correspondence.

2. LITERATURE REVIEW

Wai Kay Leong, Aditya Kulkarni, Yin Xu and Ben Leong [1] provides an analysis and some suggestion to protect our cellular data network environments from some crucial attacks like Data Loss, DOS Flooding attack and battery charge drain.

While the accessibility of an open IP address in a cell information system will permit new administrations to be sent on cell phones, it additionally presents security vulnerabilities. Author claimed to be researched three structures of IP-based assaults: (i) information portion channel, (ii) Dos flooding, and (iii) battery Loss. While ordinary DOS flooding ambushes can be viably recognized, these attacks oblige such low data rates that they are troublesome to discrete from true movement without some appearance of significant bundle evaluation. As it is not viable to expect that Internet administration supplier will offer such survey organizations to all endorsers, we suggest that an essential go-between based firewall with a secret IP area be used to deter these strikes.

To address this issue, they put an intermediary server that diverts parcels to the cell phone as represented. Once on the web, the cell phone will send a parcel to the intermediary server, consequently making a firewall rule to permit approaching parcels from IP. True blue clients can send bundles to the cell phone by sending parcels through the intermediary, and an advanced firewall with custom rule can be actualized at this intermediary to whitelist true blue activity. Then again, a genuine sender can likewise ask for a "callback" from themobile gadget, asking for the gadget to send a parcel to the sender, accordingly making a rule in the ISP firewall that will permit immediate approaching associations from the sender. Shockingly, in the same way as a NAT server, one will at present need to expressly promote the IP location of the intermediary server. In the event that an aggressor is ready to find the IP location of the cell phone, he can disguise as the intermediary server, and send pernicious parcels through the firewall, as delineated. To address this potential defenselessness, we give the intermediary a second IP address that is known just to the cell gadget. Assume the intermediary utilizes a second IP to unite with the cell phone, an aggressor, who knows just of the publicized intermediary address, would not have the capacity to take on the appearance of the intermediary regardless of the fact that it knows the IP of the cell phone. To prepare for mocking assaults steered at the intermediary, the intermediary's firewall can perform profound bundle assessment or validate the payload to check it originates from honest to goodness has. Such multi-IP intermediary servers can be actualized in a cloud administration and made accessible as a general administration to cell endorsers for an ISP.

Main Point to note down are the authors discussed about IP based attacks and the proposed the solutions but did not show and discussed about the results and effects after words.

Ping Wang, Chih-Chiang Ku and Tzu Chia Wang [2] presents a security model for the user's authentication. The model is for remote users. In the proposed approach, less piece of the biometric information is encoded and put away on a smart card, while the other comparing piece of the information is scrambled and put away on a server and creates the keys utilizing Diffie & Hellman key trade calculation.

A secret-splitting remote authentication scheme have three phases which are "initialization phase", "Registration phase", and the "Authentication phase". In the Initialization phase when the smart card maker recognizes a solicitation from the Certificate Authority, it creates distinctive security parameters into the smart cards and a while later sends the cards to the CA. The steps are as per the following:-

- Producer arbitrarily picks an extensive prime numbers
- Producer figures one of a select Authentication Number (A) concentrated around a predefined coding standard.
- Producer heedlessly picks a 128-bit string.

In the Registration phase,the client registers with the CA and gets a brilliant card once he or she has confirmed their certified character utilizing a physical personality account.The registration stage has five steps:

- Client with character be going to enroll with the server. The customer picks a card's mystery scratch, the watchword is then saved to the shrewd card, and after that secured by the encryption arrangement of smart card.
- Unique finger impression picture of User is brought with the assistance of a sensor and the subtle elements are taken out from this picture to structure a finger impression format.
- the terminal figures hashes
- the terminal sends hashes to the server on a safe medium
- the terminal stores data on the smart card

In the Authentication phase customers implant their clever card, containing a part of the way confirmation format into a card follower and a login sale is then sent to the affirmation server. The unique finger impression data is checked through the accompanying steps:-

- Customer inputs watchword into the terminal. On the off chance that the secret word is accurate, the Authentication Number is correct? Else rejected.
- Customer furnishes unique mark impression with the assistance of a sensor, and the unique mark impression is then compared with that put away data on the validation server.
- The terminal calculates the hashes of the two functions and identifies the difference. The two sections are then consolidating into one spot to create the full biometric impression of the client.
- Common session key computed and imparted among terminal and the server.
- Server delivers a one-time symmetric key and figures the message sends message to the terminal y encoding the message with the assistance of one-time symmetric key.
- Decryption methodology performs and extricates the message.
- The terminal looks at the message from both, the terminal and the server. On the off chance that there is a match, the client is successfully distinguished; else the terminal sends some message to the server for confirmation once more.
- Servers re-accept data. In the event that acceptance is there, then the server receives the login ask for overall

From this paper the authors propose a methodology not just determines the issue of information misuse by inside staff, additionally aides ensure the clients' data against malevolent assault, and for example, compromise the Certificate Authority (CA) as to fake the whole biometric data, unscrupulous staff or programmers should all the while decode two mystery keys as opposed to only one.

As per the moderators of the paper the remote verification plan focused around a mystery part idea is proposed for determining the issue of client security in cloud computing applications. Rather than existing multi-element confirmation conspires, the proposed strategy minimizes the risk of assaults by exploitative inner part representatives since just a subset of the data

needed to breeze through the live ness test is put away on the client verification database.

Apart from these, the authors of the paper haven't give the implementation framework or implementation results. Another thing is that if the finger prints impressions compromised at the start then the whole mechanism will compromise at all. Man in the middle Attack is there to know the keys between the terminal and the server, which can be a big bottle neck for the security of the proposed system.

A.Cecil Donald, A. JenisḂand L. Arockiam [3] proposes an authentication mechanism for the security enhancement in cloud premises.The proposed system for verifying the client in cloud stage. In this model, an idea of giving a Digital Signature (DS) at the client story and a Trusted Authenticator (TA) for giving high security is introduced.

This model permits the cloud client to get to the administrations from the cloud administration supplier's by validating the right to gain entrance demands. The correspondence between the client and the Cloud service provider company are validated by the Trusted Authenticator (TA). The trusted authenticator validates the client and permits the client and CSP to impart in getting to the administrations.

The TA has two stages, one was the Registration stage and an alternate was the check stage. The TA has a database server which checks for enlisted client and approves the client to get to administrations from CSP. In the event that the client is not an enlisted customer, it makes an impression on the invalid customer. The TA likewise gives an advanced mark, which gives higher security level of getting to administrations.

At the point when the client gets accepted, he is allowed to approach the CSP for requesting the administrations alongside the Digital Signature. The program on the client side has an extra which creates the Digital Signature of the same accreditations in which the TA produces, and the Digital Signature wraps the client demand. The client demands for getting to administrations alongside Digital Signature will be sent to the CSP.

The clouds of CSP have the solicitation from the client side and the DS from the TA and distribute the regarded CSP which has the asked for administrations. The regarded CSP has operators who confirm the DS from both client and CSP. On the off chance that they are equivalent, then the client is permitted to get to the administration effectively.

The key point to be focused in this paper by the authors are that the authors didn't provide implementation frame work and implementation results. They also not discussed about communication mechanisms between user, TA and CSP. As if the data, during transmission, is during modified or scrambled, then whether the whole process will start from start or something else. Neither discussed anything about TA system nor about CSP.

Daniela Elena Popescu, Alina MadalinaLonea [4] discusses a model to authenticate a user with the help of image and text. They call it image & text based hybrid authentication system to get cloud services.

The framework comprises of aAuthentication server (AS), and a Authenticated Use Agent (AUA) and it obliges that the client have appointed a subset of pictures (as passwords) from a bigger set. The set of all pictures utilized by the Image Based Authentication (IBA) framework, named picture set, contains pictures that are different to the human eye, they are not effectively describable and they contrast in structure.

To perform stronger verification for getting to the cloud administrations, they propose to utilize a validation plot that performs the accompanying steps:

1. Make a content built confirmation situated in light of the client ID and a content watchword to have entry to the cloud administrations

2. Make a mixture content picture based validation that uses our own proposed answer for verification; it joins the pictures with content and is a decent answer for staying away from the animal energy assaults and to guarantee a solid confirmation plan

3. Utilize the X.509 guidelines for acquiring the client certifications

The next step from the validation plan assume that when the client will enlist into the cloud administration, he/she will get an arbitrarily network of pictures. Every framework of pictures will contain 3 pictures and each one picture will have a relating number.

The client will need to give a mystery code to each one picture. In this sense, the client will get an enrollment structure, where it is approaching to present mystery characters for each one comparing number.

After the client presented their particular mystery code for each one relating picture, the enrollment will be figured it out. The client ought to recall which code he/she had accommodated each one kind of picture, in light of the fact that the proposed confirmation strategy obliges entering these codes, yet each one time the pictures will be connected with diverse numbers (from 1 to 3), in light of the fact that the numbers are created utilizing a stage calculation. In this way, for verification strategy there will be the same pictures each one time, however with an alternate comparing numbers.

In this paper authors gave combination of text and image based system for the authentication of the users but did not implement on practice grounds. Did not provide implantation frame work and implementation results.

3.RESEARCH METHODOLOGY

The methodology adopted for this research required problem statement and identification. Then identify the components involve during the lab-work, make the simulation. After that implementations and calculations to develop the model for improvement and secure user authentication in cloud computing.

The components of the models that involve in the implementation of the model are as under. The description of the components is also added with.

Virtual Private Network (VPN) is a get-together of machines (or discrete frameworks) sorted out together over an open framework particularly, the web. Associations use VPNs to interface remote datacenters, and individuals can use VPNs to get access to framework resources when they're not physically on the same LAN, or as a procedure for securing and encoding their correspondences when they're using an untrusted open framework. When you join with a VPN, you ordinarily dispatch a VPN client on your machine, log in with your accreditations, and your machine exchanges trusted keys with a faraway server. When both machines have affirmed each other as genuine, the larger part of your web correspondence is mixed and secured from listening in.

It secures your machine's web relationship with guarantee that most of the data you're sending and getting is encoded and secured from prying eyes. Whether the VPNs you're familiar with are the ones offered by your school or business to help you work or stay joined when you're voyaging or the ones you pay to get you watch your most cherished shows in an interchange country as they air, they're all doing moreover thing.

Secure Socket Layer (SSL) is a machine organizing convention that oversees server validation, customer confirmation and encoded correspondence in the middle of servers and customers. SSL utilizes a blend of open key and symmetric-key encryption to secure an association between two machines, commonly a Web or mail server and a customer machine, imparting over the Internet or an inward system. Utilizing the OSI reference show as setting, SSL runs over the TCP/IP convention, which is in charge of the vehicle and steering of information over a system, and underneath more elevated amount conventions, for example, HTTP and IMAP, encoding the information of system associations in the application layer of the Internet Protocol suite.

IP Security (IPsec) is the most secure technique monetarily accessible for interfacing system destinations. IPsec wasintended to give the accompanying security characteristics when exchanging signal packets crosswise over systems. IPSec has three salient and most important features in terms of security. These are **Authentication which v**erifies that the signal packets got is really from the guaranteed sender.

Integrity which ensures that the substance of the parcel did not change in travel. **Confidentiality which** conceals the message content through encryption.

Virtual ServersA virtual machine is an item machine that, in the same route as a physical machine, runs a working structure and applications. The virtual machine is contained an arranged of subtle element and plan records and is backed by the physical resources of a host. Every virtual machine has virtual devices that give the same value as physical fittings and have additional focal points the extent that reduction, sensibility, and security. A virtual machine contains a couple of sorts of reports that you store on an upheld stockpiling device.

3.1 Problem Statement

As Cloud computing has emerged as a vital role in today's world of computer sciences and IT. It provide resources, storage, applications etc. as user required without any physical implementation by the end user. The user just put the requirements and get what he/ she demands. There are three basic implementation models of cloud which are Saas, Paas and Iaas. Software-as-a-Service (Saas) provide an opportunity of its user to provide all required softwares at one single place. Any user who is legitimate to user that service, can use that softwares as and when required from any place. Platform-as-a-service (Paas) provide an opportunity to have platform over the internet or intranet which is needed for the business needs. That platform will have all the required things which are user demanded. That platform can be for the development or for huge data analysis, it doesn't a matter of concern for the cloud service provider. The next is Infrastructure-as-a-Service (Iaas), provide infrastructure to its users. The infrastructure could be for storage, networks or to implement some specific applications by the user.

The end user can get the services by just register itself and then get the services. User must get authentication from the cloud service providing company before getting the service. After being authenticated by the cloud service provider company, a user can get in to the cloud premises and can do everything for which he /she is allowed to do.

During studies about authentication in cloud premises, we choose these problems to be work for. These two problems are as follows:-

3.2 Problem Identification

*Servers are directly accessible:-*Server security is as critical as system security in light of the fact that servers frequently hold a lot of an enterprise's key data. On the off chance that a server is traded off, every last bit of its substance may get to be accessible for the aggressor to take or control freely. The accompanying areas detail a portion of the principle issues. An enterprise's servers give a wide mixed bag of administrations to inward and outside clients, and numerous servers likewise store or methodology touchy data for the association. Likely the most broadly perceived sorts of servers are Web, email, database, framework organization, and record servers. This dispersion addresses the general security issues of customary servers. Servers are frequently concentrated by aggressors because of the estimation of their data and organizations. For example, a server may contain eventually identifiable data that could be used to perform information extortion. The going with are examples of basic security dangers to servers: Harmful components may misuse programming bugs in the server or its shrouded working system to expansion unapproved access to the server. Refusal of organization (DOS) attacks may be controlled to the server or its supporting framework base, denying or blocking considerable customers from making usage of its organizations. Unstable information on the server may be examined by unapproved individuals or changed in an unapproved way. Delicate information transmitted decoded or weakly encoded between the server and the client may be gotten. Malevolent substances may expand unapproved access to resources someplace else in the undertaking's framework through a viable ambush on the server. Pernicious substances may attack diverse components in the wake of exchanging off a server. These strikes can be impelled direct (e.g., from the bartered host against an external server) or in an indirect manner. (e.g., setting vindictive

substance on the traded off server that endeavors to adventure vulnerabilities in the customers of clients getting to the server).

As the cloud resides on the internet so the servers, involve in providing cloud service are accessible to the users. Users get connect to users and request for the authentication. If that server authenticates a user, then that user will enter and use the cloud services otherwise not. The question here if that server is compromised by brute force attack or anything like this or be victim of DOS/DDOS, then the user will be authenticated and cloud services will not be provided to the users. So the servers who are providing authentication or the service provider servers must not be exposed on to the internet and the users must pass through the authentication process before get in to the DMZ. So servers obviously have the key role in providing services and servers must not be exposed directly to the users or customers.

Live IP addresses: - As we all know the importance of a live IP address. Live IP address gives the actual system or device IP address. The device may be a single device, a server or gate way to the network. It is also important that many of the applications works on the live IP addresses. If the actual live IPs are exposed on the internet, then this could be dangerous.

The essential convention for sending information over the Internet system and numerous other machine systems is the Internet Protocol ("IP"). The header of every IP parcel contains, in addition to everything else, the numerical source and boundary location of the bundle. The source location is ordinarily the address that the parcel was sent from. By producing the header so it contains an alternate address, an aggressor can make it create the impression that the parcel was sent by an alternate machine. The machine that gets ridiculed bundles will send a reaction again to the manufactured source address, which implies that this system is predominantly utilized when the assailant does not think about the reaction or the aggressor has somehow of speculating the reaction.

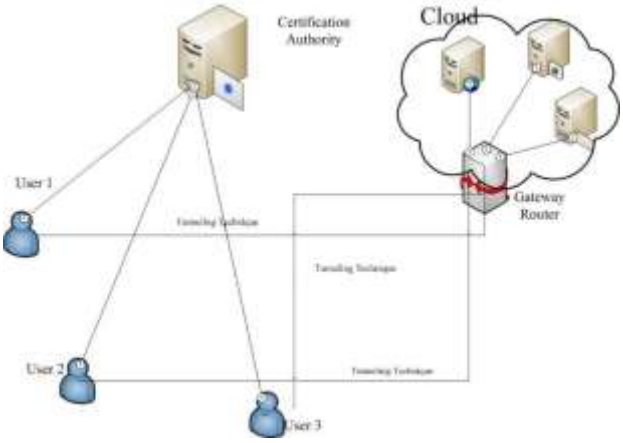
3.3 Proposed Model

The main idea of the model is to authenticate a user before entering the cloud premises. At the door of the cloud, a user must authenticated and then enjoy the cloud services. To do this we have limited the UN-authenticated users' to the door of the cloud and within the cloud, there is no one who is unauthenticated. The bad guys generate unnecessary traffic within the cloud and can launch different types of attacks. If a user is not correct one, he must use the cloud services and if the user is an authenticated user and have correct credentials to get into the cloud then he must enter in to the cloud and use the cloud services for which he pays. Currently, when a user enters the username and password, the server checks it in its database whether it is authenticated user or not and every time server will refuse the un-authenticated users. What will as server do if a bad guy gives wrong credentials to the server again and again, and the server checks every time his credentials, whether the credentials are correct or not. By doing this, a sever may be a victim of DOS or DDOS attack. Same is the case, if a user has the live or actual IP of the service providing server, then the bad guy launch any type of attack like IP spoofing or chokes the network infrastructure. As the cloud is for all, so internet is full of notorious users so that servers can be victims of DOS or DDOS etc. Due to this cloud management infrastructure and the servers which are actually giving the services both are involve in this system and lost the resources for nothing. These resources can be used for some valuable tasks or authenticated user can use these resources in a good manner. Model here is if a user authenticate before entering into the cloud then we can save lot bandwidth which use by the notorious users. And also we keep our servers safe. Doesn't matter we have and Iaas, Paas, or a SaaS, the model will give an optimal solution for the cloud.

The proposed model can be explained into following steps. The steps are as under:-

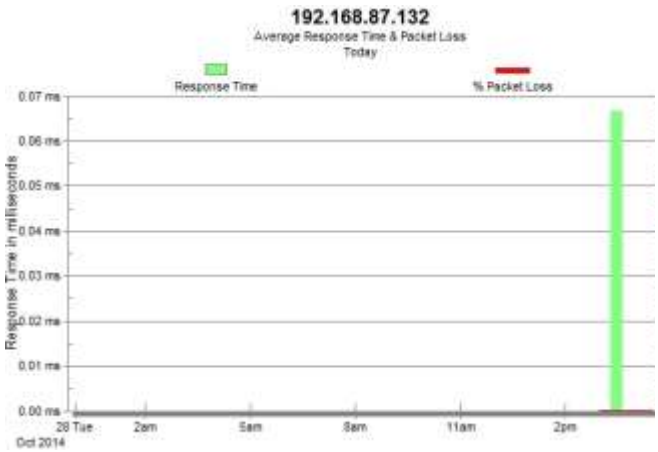
1. User requests for the security certificate.
2. User receive the security certificate and the hash of it.
3. User then encrypt the security certificate and the hash and send to the gateway router for authentication.

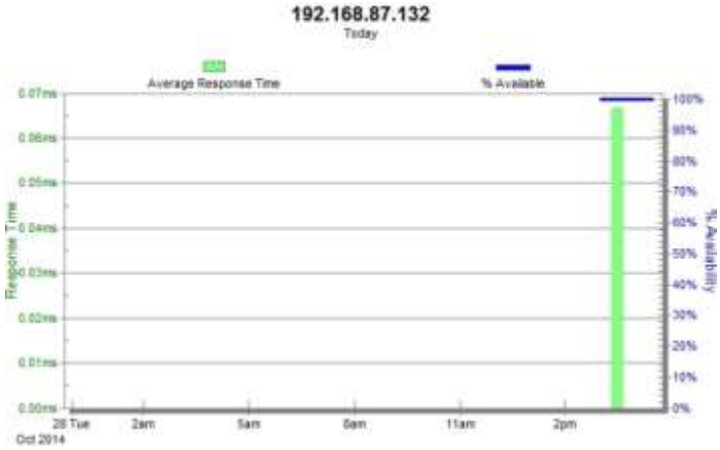
4. Gateway router decrypt the packet and gets the security certificate and hash.
5. Gateway router verifies the authenticity of the user by verifying the hash.
6. If gateway router verifies the hash, the user is an authenticated user otherwise there is a modification during communication or the user is illegitimate.
7. If the user is authenticated, the user get connected to the servers and gets the services of the cloud.
8.



3.4 Implementation and Results

The proposed model implemented and checks the performance. After implementation, the graphs shows the results of the implemented model.





4. CONCLUSION AND FUTURE WORK

The suggested model gives us security of the network infrastructure and for the servers. The cloud infrastructure, whether it is servicing as an Iaas, Paas, or Saas, has the critical resources for the enterprise so the assurance of the security of the cloud is mandatory.

The proposed model, on evaluation, gives us the following benefits from the existing models. These are as under:-

- *Hiding live IP addresses:*-By hiding the IP addresses, the infrastructure will be save from attacks form the open internet. The proposed model doing so.
- *Servers are not directly accessible:*- As for giving the services, the users are commonly directly taken the services from the servers like authentication, authorization or any type of storage accessibility etc. This can be very harmful for the services provider company.
- *Valuable bandwidth save:*-It will be more valuable in the case of cloud when each users is paying for what he wants. Each users requires the service in full capacity. If UN-authenticated users uses the major portion of the bandwidth then the authenticated users or the legitimate users have nothing in the bandwidth. Consequently they also will have to suffer for the service they wants. The proposed model gives that a user will first show his / her legitimacy, then use the services of the cloud and UN-authenticated users will limited to the edge of the cloud.

- *Time to access the services are very much low*:- The servers are not directly accessible to the users and only accessibility by authentication, as mentioned in the proposed model, so time required to access the services of the cloud will be very low. This is because of that, UN-authenticated users and illegitimate users are blocked at the door of the cloud. So the services of the cloud will provide with full capacity.
- *Response time high*:-The proposed model evaluates that the response time to deliver the services to the legitimate users is very low. The proposed model combines different techniques in a way that gives the security optimization along with the improvement in the response time.
- *Improve the Quality-of-service*: - Hiding live IPs, servers are not directly accessible, less response time etc. shows the quality of service provided by the proposed model.
- *Excludes form different types of attacks on IP addresses*: - As the live IP addressed are hide in the proposed model, so the proposed model gives the security model with less attacks on the live IPs like DDOS/DOS.
- *Security ensure with tunneling technique:* - There are different types of tunneling techniques in the world of computer network. There are also many tunneling techniques use to implement security in the infrastructure. So security implemented through tunneling technique is a recommended way to implement security in the cloud.
- *Improvement in efficiency and productivity of cloud performance*:- By all these ways, there is improvement in the efficiency and the productivity of the cloud's performance. The security implementation through the proposed model gives the cloud setup more secure, more efficient and more productive.
- *Theft of client device*: - If a client get physical access to the customer gadget – e.g. handset, and wishes to utilize this as a part of a way that advantages him. He may wish to erase critical documents for unique client distributed storage, perform installments, access individual information, or just turn into the new client of the customer gad
- Future work involve the improvements in the efficiency, response time and security with the expansion in the cloud environment.

5 REFERNCES

[1]Wai Kay Leong, Aditya Kulkarni, Yin Xu and Ben Leong, "Unveiling the Hidden Dangers of Public IP Addresses in 4G/LTE Cellular Data Networks", Proceedings of the 15th Workshop on Mobile Computing Systems and Applications, Article No. 16, February 2014

[2] Ping Wang, Chih-Chiang Ku and Tzu Chia Wang, "A New Fingerprint Authentication scheme based on Secret-splitting for Cloud Computing Security, Recent Application in Biometrics" JULLY 2011Available at: http://www.intechopen.com/books/recent-application-in-biometrics/a-new-fingerprint-authentication-scheme-based-on-secret-splitting-for-cloud-computing-security,.

[3] A.CecilDonaldȦ*, A. JenisḂand L. ArockiamĊ, "An Authentication Mechanism to Enhance Security in the Cloud Environment", International Journal of Current Engineering and Technology, Vol.4**, No.5 (Oct 2014)**

[4]Daniela Elena Popescu, Alina MadalinaLonea, "**An Hybrid Text-Image Based Authentication for Cloud Services**", **International Journal of Computers Communications & Control (IJCCC), April 2013, www.http://univagora.ro/jour/index.php/ijccc/article/view/307**

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.