ISSN: 0976-3104
SPECIAL ISSUE: Emerging Technologies in Networking and Security (ETNS)

THE IIOAB JOURNAL

ARTICLE OPEN ACCESS

A STUDY OF PROTOCOL SECURITY -CLOUD ARCHITECTURE

Sabapathi*, Muniyappan, Danu Senthil
Dept. of CSE, Vel Tech High tech DR.RR&DR.SR Engineering College, INDIA

ABSTRACT

Aims: *Protocol security which is important concern in the network security, which ensures the security and integrity of data transmission over the internet. Secure network data from any illegimate attempt to extract content of the data and Cloud Computing is the advance computing technology for the internet users.* ***Materials and methods:*** *We can enhance our system without modify or changing our resources by the internet over cloud technology .So, all the resources we can get through cloud system. Our data should be transmit in secure channel.* ***Results:*** *This paper focus on Protocol security in private cloud system deployment and security against POODLE (Discovered by GOOGLE TEAM at OCT 2014).*

Published on: 10th– August-2016

KEY WORDS

Private Cloud, POODLE, ECC and DH, Open Stack

***Corresponding author: Email:** sabapathi2000@gmail.com **Tel.:** +91-95008-25476; **Fax:** +91-44-26840 249

INTRODUCTION

Protocol security, Protocol it's the set of rules which act as channel for connectivity for the data transferring. So, it's a important concern on connection setup over network. For secure communication, in cloud system, it's much more important. SSL (Secure Socket layer), is a protocol used to transfer the private encrypted data and deliver through the secure communication. Two sub protocols were exists in SSL, they are Record and Handshake protocol. When the data transfer, then the format is called Record protocol, and the exchange between client and server are done using the record protocol, which refers as handshake protocol. Cloud computing, Resource centric technology; we can access the resources over the network. Through Cloud computing, Centralization of infrastructure with low cost, we can increase the Peak –load capacity, dynamic allocation of CPU, storage and bandwidth.Virtualization,running multiple Operating System on single physical computer. So all the resources, we can get via Cloud technology. If we get software like Ms –Office from the cloud then it's called Software As A Service (SAAS).If Operating system provide service Platform As A Service (PAAS), If it's resources provide service like storage then it's called Infrastructure As A Service (IAAS).POODLE (Padding Oracle On Downgraded Legacy Encryption), it's Protocol secure break vulnerability on SSL V3.POODLE it's a Man –In –The Middle attack, which is exploit and allows attacker to read cipher text So Against POODLE we useTLS_FALLBACK_SCSV,It's a tool using TLS 1.2.OpenStack, it's a Cloud Operating system and its set of software tools for building and managing cloud computing platforms for public and private. Actually OpenStack it's a open source software .HTTPS/TLS 1.2 connection setup, Private cloud deployment using OpenStack, Elliptic Curve Cryptography and Diifie Hellman using for short key generation and secure connection establishment.

RELATED WORK-EXISTING PROBLEM

We should analyses the communication channel eavesdrops Https/SSL channel has lot of Man in the Middle Attacks are possible. If I connect to the banking via the Wi Fi ,we may think our connection is secure but the Wi-Fi hotspot might connect to bank behalf of ourselves.Wifi hotspot sneakily redirect to an Http page and connect to the bank ,eavesdrop may threat our transaction details. other way "Homographic similar https address" and SSL doesn't have perfect forward secrecy SSL connection Andsome establishes two main phases, handshake and secure data transfer phases. This paper should not be against of SSL but we should aware of associated problems with SSL. Private Cloud setup OpenStack can explore with help of the Mass Phishing, brute force and automated exploitation tools there are lot of open source cloud solutions are available to build private cloud with IaaS cloud service layer. Vorasetal. [1] Devises a set of criteria to evaluate and compare most common open source IaaS cloud solutions. Mahjoubet al. [2] compares the open source technologies to help customers to choose the best cloud offer of open source.Technologies. Most common open source cloud computing platforms are scalable, provide IaaS, and support dynamic plat-Form, Xen virtualization technology, Linux operating system and Java [3],[4]. However, they have different purposes. For example, Eucalyptus [5] fits well to build a public cloud services (IaaS) with homogeneous pool of hypervisors, whileOpenNebula [6] fits well for building private/hybrid cloud with heterogeneous virtualization platforms [7].Many authors have analyzed the cloud security challenges and propose methodologies for security evaluation of theCloud solutions. Cloud Security Alliance (CSA) announce Cloud Control Matrix Version 1.3 [8] which can assistthe potential cloud customers to assess the overall security risk of a cloud service providers classifying the security Controls according to cloud service layer and architecture. Methodology for security evaluation of on-premise systemsand cloud computing based on ISO 27001:2005 [9] is pro-posed in [10]. The authors in [4] evaluate ISO 27001:2005Control objective importance for on-premise and the three cloud service layers IaaS, PaaS (Platform as a Service) andSaaS (Software as a Service). International Organization for Standardization (ISO) is developing new guidelines ISO/IECWDTS 27017 [11] that will recommend relevant security controls for information security management system(ISMS) implementation in cloud computing. Eucalyptus and CloudStack [12] have integrated the maximum security levelin front of Open Nebula and OpenStack open source cloud solutions [13].

SYSTEM AND MODELS

Our system model involves cloud service provider which includes cloud system administrators, tenant administrators n (or operators) who manage the tenant virtual machines, and tenant users (or tenant's customers) who use the applications and services running in the tenant virtual machines. Cloud providers are entities such as Amazon EC2 and Microsoft Azure who have a vested interest in protecting their reputations. The cloud system administrators are individuals from these corporations entrusted with system tasks and maintaining cloud infrastructures, who will have access to privileged domains. In our proposal we usingOpenStack as a private cloud system, which controls the large pool of computing, storage, networking resources via the user friendly interface. Openstack has more features such as rolling upgrades, federated Identity service. We assume that as cloud providers have a vested interest in protecting their reputations and resources, the adversaries from following modules.

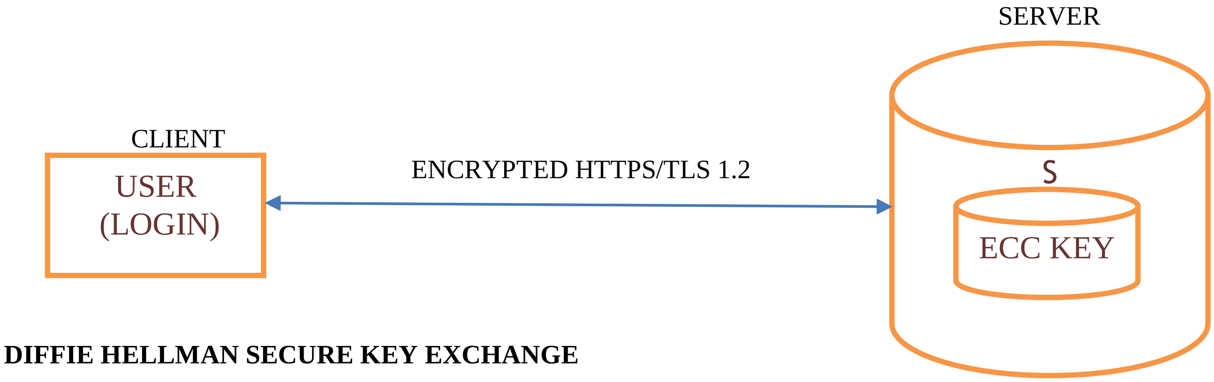


Fig: 1. INTERNAL PROCESSING MODEL– CLOUD SYSTEMS

………

In Secure cloud systems should use secure channel for data transfer. In this proposal mainly for against for the POODLE .POODLE it's a kind of Man in the Middle Attack, which can disable Https/SSL base connection. In this connection we have usingencrypted Https/TLS v1.2 **[Figure -1]** shows channel, when the user login to the browser and sends the request to the server, then the server generated key using elliptic curve cryptography and safely handover the key with response using Diffie Hellman secure handshaking methodology to the user. Hence the channel should be encrypted Https/TLS v1.2 against POODLE concern.

METHODs

System Design Model

In our proposedsystem, we tried full fledge integrity and more secure concern model over the networking system and we designed in private cloud platform of OpenStack .In our secure model provide overall the starting level of communication channel to the end level. Starting from user account creation for the login, account form have more peculiar details query. All the peculiar data stored in the server. The password will be generating by the server, that password should be stronger and individual can remember their password easily and stronger. For example my last name ix Birth year is 1989, grandfather name is subramani,my, my favorite symbol is $,then the password may mani89$x.So that if I lost my physical id saved thing like my mobile,pendrive,wallet like except mymemory, the authentication threat like guessing password vulnerability may prevent. Then the Encrypted Http/TLS v1.2 protocol base connection setup against for POODLE attack, then local server designed as using OpenStack as a cloud base local server. In Openstackinbuild component Keystone also provides the very good authentication additionally deploying ECC base key generating in the OpenStack. Once the Shortest and strong key generated then the key safely transferred to the client via Secure Diffie Hellman Handshaking protocol. In this paper we define five modules, are following

Entry Module

User Account creation shouldbe more specific, peculiar, ultimate details collection. Based upon of the uniquedetails, the password will be generated. Because of the key should be more unique. Because password guessing hacking or some may lost their ID Proofs, then hacker may try to illegal usage of your account. For example if I lost my wallet within that National ID's. Then hacker tries to guessing password. Once they get, they may the king of your things. Sothat, strong password should be more required. So that Account creation should have psyche identity, personal interest, National Id proof, Grandfather Name, like. Password should more specific, if hacker try the forget password options, they should get more trouble.

SEO Analysis For Seeking Secure Protocol

Channel Communication is the more important aspects in the networking system.So,that protocol plays the vital role in the security part, in recently POODLE attack which causing the SSL disability. So Protocol seeking in our system which should more secure and supports more website visibility. In this connection, we Analysis gives the secure channel, reliability, protocol. As per SEO Report encrypted Https will give more optimized for our model. Statistical **[Figure -2]**] Shows, encrypted Https will give standard visibility for the net users. In blackline represents the encrypted Https and and shadowed represent the http users. Significantly increasing the encrypted Https users because of which supporting more number of website.

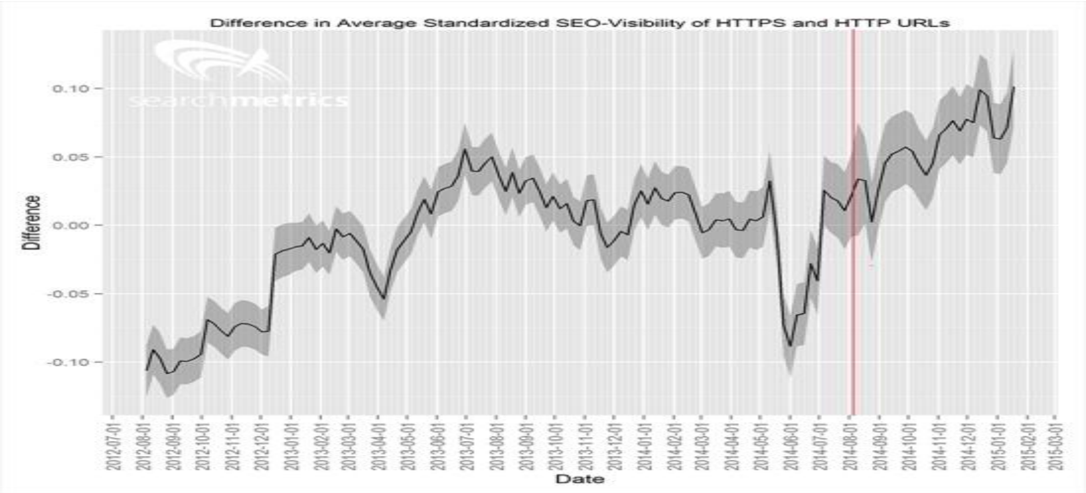


Fig: 2. Https significantly increase their visibility As SEO Report

....

b.iConnection Setup viaencrypted HTTP-TLS v1.2

Communication channel has more important concern securing network. WhereverHTTPS/SSLV3, there isPOODLE, Wi-Fi hotspot, likewise more MITM attacks are associated with SSL.In the POODLE (Padding Oracle Downgraded Legacy Encryption), it will disable the SSL base connection and threat the confidential things. Initially used in cloud setup for connection establishment. Hence SSL 3.0 will disable by the POODLE Hacker.

THE IIOAB JOURNAL ISSN: 0976-3104

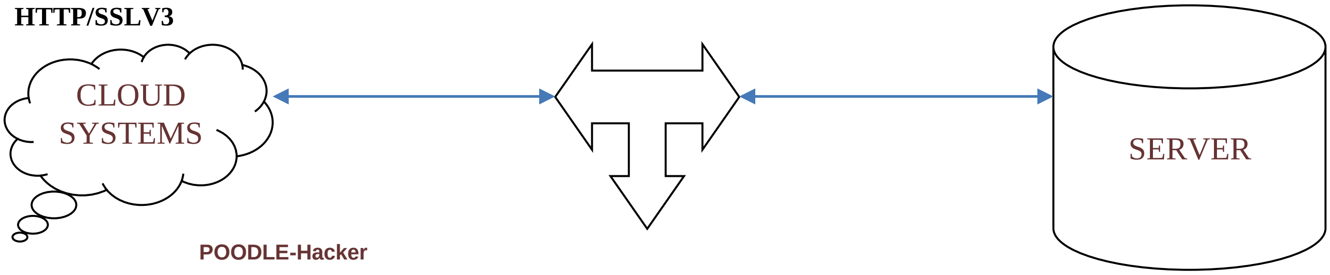


Fig: 3. POODLE –Exploit SSL v3

So that in our proposed system client and server communication channel using encrypted HTTPS/TLS v1.2 were we used for against POODLE. **[Figure -3], [Figure -4]**

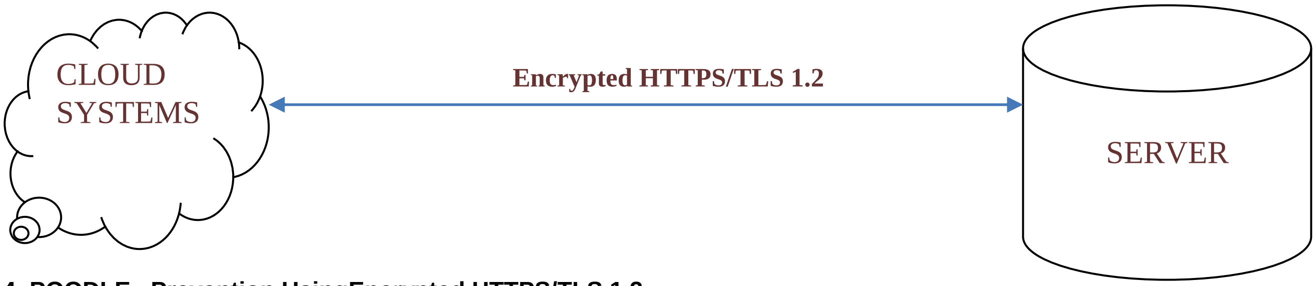


Fig: 4. POODLE –Prevention UsingEncrypted HTTPS/TLS 1.2

Server Authentication

We examined in cloud system. In this project deploy OpenStack- private cloud act as local server .Openstackis an Open source cloud platform. Openstack has the set of software that can manage the cloud environment. Openstack, OpenNebula like lot of open sources are availbale.So anyone can add components to OpenStack to help it to meet their needs. Openstack has set of components some of them follow.

OpenStack **[Figure -5]** provides the very good support for protocol security and efficient way of private cloud platform**.**

NOVA-Primary computing engine behind Open stack. It's a fabric controller which is used for deployment and managing virtual machines and computing tasks.
SWIFT – Storage system for object files. This makes scaling easy**.**
CINDER – block storage component
NEUTRON – Networking capability for OpenStack
KEYSTONE –Provide Identity Service for authentication and authorization
HORIZON – It's a Dashboard behind OpenStack. It's a modular web based User Interface (UI)
CEILOMETER –Provide single point of contact for billing system.
HEAT- Provide Orchestration services for multi composite cloud applications**.**
TROVE- Provide Database as a service

Unique ID Generating

Client establishes the connection using Http/TLS 1.2 to the OpenStack local server. The server has generate the key Using Elliptic Curve Cryptography, we can generate the around 160 bits providing same security level as 1024 bits. So that Computation speed is high. Less Memory, long term battery life. So ECC will generate key efficiently.ECC will give the good support to the ECC and DH[14].Based on National Institute and Standard Technolgy table comparison with their ratio Recommends **[Table- 1],** we used Elliptic Curve cryptography foe short and speedy key generation.

THE IIOAB JOURNAL
ISSN: 0976-3104

Key Exchange

Password authenticated key management ((PK) in the form of Secure Diffie Hellman (DH) key exchange algorithm was secure key transfer.PK DH It's a Public key cryptography .It uses two keys, for sending message to server using with private key and server responses via the public key. Receiver side using his private key fordecrypt and response using the public key. DH for secure Handshaking, connection establishes supports.

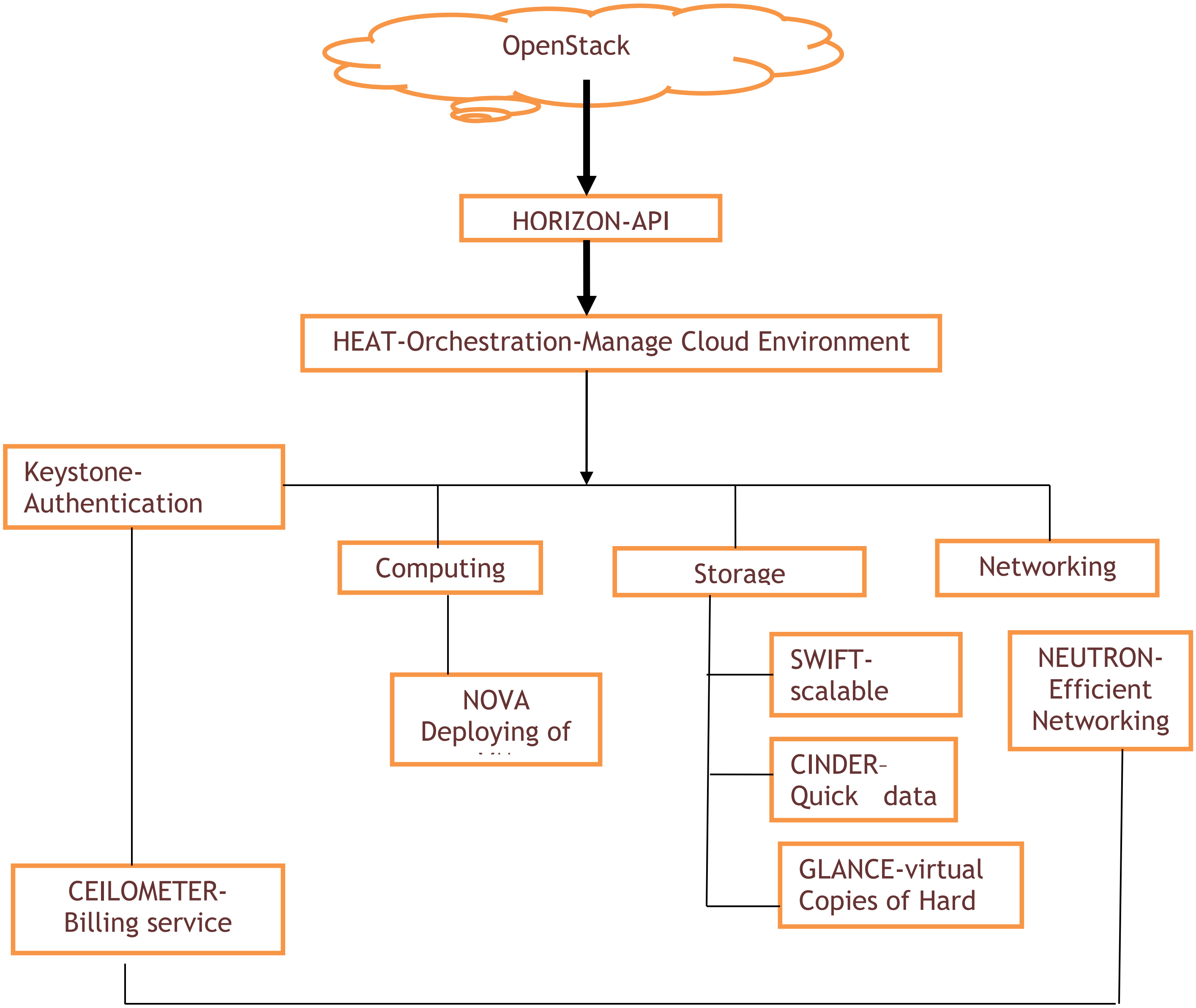


Fig: 5. Open Stack Components

THE IIOAB JOURNAL ISSN: 0976-3104

RESULT AND DISCUSSION

TLS provide very good supporting for secure channel of communication against eavesdropping, and MITM attacks.

WEBSITE SUPPORT

Table: 1. PROTOCOL WEB SUPPORT AND SECURITY ANALYSIS

Protocol Version	Website Support	Security
SSL 2.0	10.4%	Insecure
SSL 3.0	32.6%	Insecure
TLS 1.0	47.2%	GOOD
TLS 1.1	65.7%	Good
TLS 1.2	69%	Very Good

Moreover TLS 1.2 connection setup, website supports are significantly increasing in the Search Engine Optimization world. Protocol support in security [16] are very essential.

We uploading the malware via http to the server, then the malicious Http uploading was detected, but the encrypted HTTPS exploit the malware. Https supporting significantly increase the websites support [15], overall the network and the TLS v1.2 provide more secure and reliable to the protocol security. So in our system we tried to use encrypted https and TLS v1.2 for secure communication channel. As per SEO Report encrypted Https will give more optimized support overall the network and the TLS v1.2 provide more secure and reliable to the protocol security. So in our system we tried to use encrypted https and TLS v1.2 for secure communication channel. In Server part, we concerning short and strong key generation so that ECC algorithm which helps, more memory and time saving. After Key generation which should safely handover to the client using the Diffie Hellman Handshaking protocol

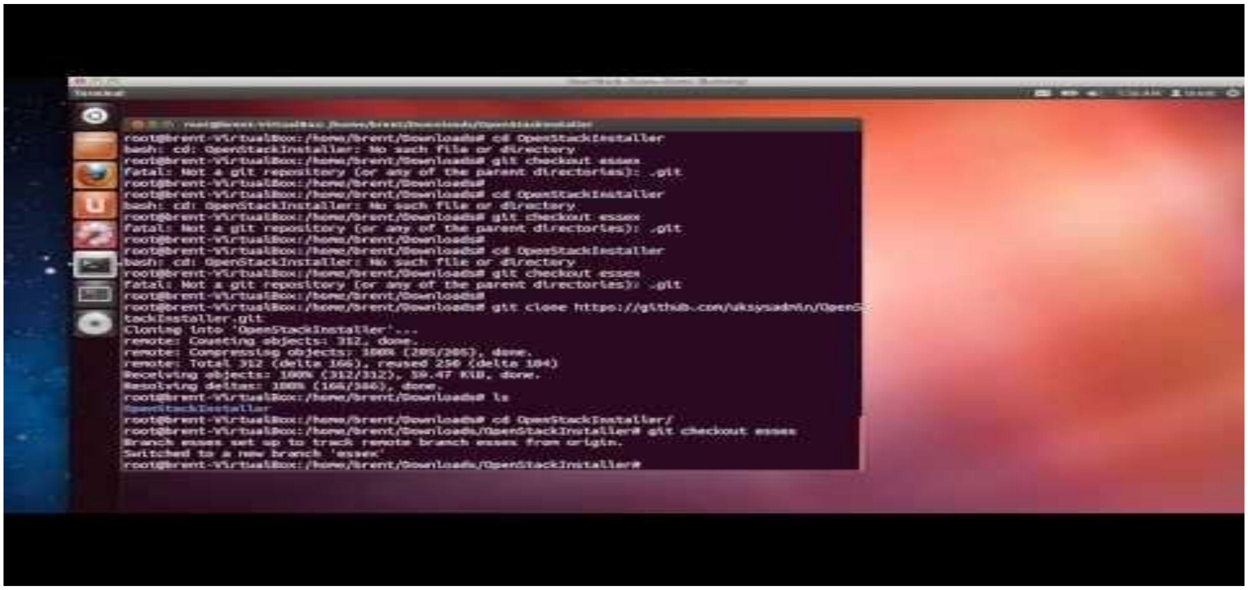
Output

Table: 2. ECC&RSA Key Comparison

Symmetric Key Size(bits)	RSA& DH size(bits)	Elliptic Curve Crypto Graph& DH Key & Size(bits)	RSA&ECC Ratio
80	**1024**	**160**	**7:1**
112	**2048**	**224**	**14:1.5**
128	**3072**	**256**	**21:2**

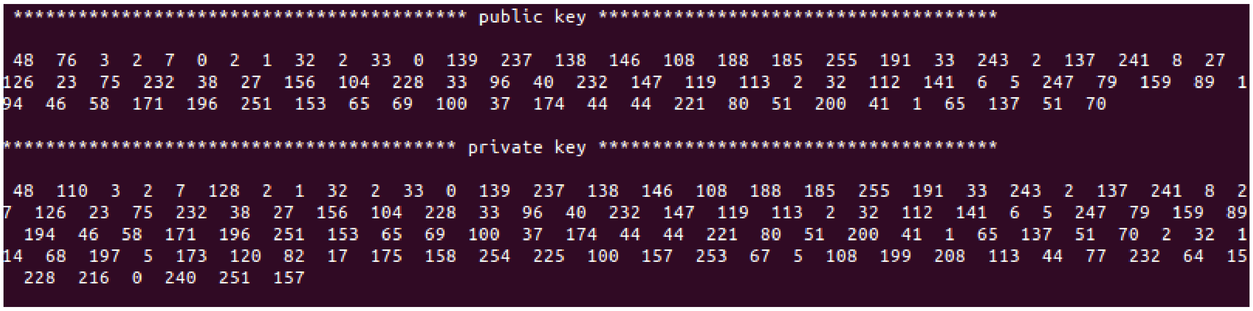
This output shows comparatively RSAVsECC key generation ratios are shown as **[Table- 2]**.So that ECC&DH combination will gives more secure transmission, short and secure key generation is possible. As per SEO reports Encrypted Https/TLS v1.2 supports, OpenStack Keystone authentication in server side ,then the Elliptic Curve cryptography and Diffie Hellman Secure handshake will provide more strengthen towards the data transmission and secure system

Screen Shot



```
root@brent-VirtualBox:/home/brent/Downloads# cd OpenStackInstaller
bash: cd: OpenStackInstaller: No such file or directory
root@brent-VirtualBox:/home/brent/Downloads# git checkout essex
fatal: Not a git repository (or any of the parent directories): .git
root@brent-VirtualBox:/home/brent/Downloads#
root@brent-VirtualBox:/home/brent/Downloads# cd OpenStackInstaller
bash: cd: OpenStackInstaller: No such file or directory
root@brent-VirtualBox:/home/brent/Downloads# git checkout essex
fatal: Not a git repository (or any of the parent directories): .git
root@brent-VirtualBox:/home/brent/Downloads#
root@brent-VirtualBox:/home/brent/Downloads# cd OpenStackInstaller
bash: cd: OpenStackInstaller: No such file or directory
root@brent-VirtualBox:/home/brent/Downloads# git checkout essex
fatal: Not a git repository (or any of the parent directories): .git
root@brent-VirtualBox:/home/brent/Downloads#
root@brent-VirtualBox:/home/brent/Downloads# git clone https://github.com/uksysadmin/OpenS
tackInstaller.git
Cloning into 'OpenStackInstaller'...
remote: Counting objects: 312, done.
remote: Compressing objects: 100% (205/205), done.
remote: Total 312 (delta 166), reused 250 (delta 104)
Receiving objects: 100% (312/312), 59.47 KiB, done.
Resolving deltas: 100% (166/166), done.
root@brent-VirtualBox:/home/brent/Downloads# ls
OpenStackInstaller
root@brent-VirtualBox:/home/brent/Downloads# cd OpenStackInstaller/
root@brent-VirtualBox:/home/brent/Downloads/OpenStackInstaller# git checkout essex
Branch essex set up to track remote branch essex from origin.
Switched to a new branch 'essex'
root@brent-VirtualBox:/home/brent/Downloads/OpenStackInstaller#
```

Openstack installation



```
 ****************************************** public key ***************************************

 48  76  3  2  7  0  2  1  32  2  33  0  139  237  138  146  108  188  185  255  191  33  243  2  137  241  8  27
126  23  75  232  38  27  156  104  228  33  96  40  232  147  119  113  2  32  112  141  6  5  247  79  159  89  1
94  46  58  171  196  251  153  65  69  100  37  174  44  44  221  80  51  200  41  1  65  137  51  70

****************************************** private key ***************************************

 48  110  3  2  7  128  2  1  32  2  33  0  139  237  138  146  108  188  185  255  191  33  243  2  137  241  8  2
7  126  23  75  232  38  27  156  104  228  33  96  40  232  147  119  113  2  32  112  141  6  5  247  79  159  89
  194  46  58  171  196  251  153  65  69  100  37  174  44  44  221  80  51  200  41  1  65  137  51  70  2  32  1
14  68  197  5  173  120  82  17  175  158  254  225  100  157  253  67  5  108  199  208  113  44  77  232  64  15
  228  216  0  240  251  157
```

Key Generation

CONCLUSION

In this paper, we propose Protocol Security using TLS 1.2 in the private cloud system against POODLE attack. In this model concern on design more secure channel communication, Registration Login form with more unique details collecting from user, Unique USER ID generation, Search Engine Optimsation Analysis for the secure protocol for the proper and secure communication channel, OpenStack Private local server, short and strong password generation using Elliptic Curve Cryptography, finally that secure key handover to the client with the help of Diffie Hellman handshaking protocol.

FUTURE ENHANCEMENTS

We examined in Private cloud system. We try to exploits multi vulnerability attacks like POODLE, Password Guessing vulnerability, And if user forget the password or Loss his ID proof hacker may attack .In OpenStack private cloud deployment then default secure keystone authentication takes place and ECC algorithm for small and speedy unique ID and key is generating. DH for secure handshaking key transfer between user and server. Overall discuss and propose secure model for private Cloud System.ln future we can move some public server security system. Security is the first and foremost for all things.

CONFLICT OF INTEREST

The authors declare no conflict of interests.

ACKNOWLEDGEMENT

None

FINANCIAL DISCLOSURE

The authors report no financial interests or potential conflicts of interest.

REFERENCES

[1] Voras B Mihaljevic, and Orlic M.[2011]Criteria for evaluation of open source cloud computing solutions, in Information Technology Interfaces (ITI), Proceedings of the ITI 33rdInternational Conference on, june 2011, 137 –142.

[2] Mahjoub M, Mdhaffar A, Halima RB, Jmaiel M.[2011]A Comparative study of the current cloud computing technology-gies and offers," in Proceedings of the 2011 First International Symposium on Network Cloud Computing and Applications,ser. NCCA '11. Washington, DC, USA: *IEEE Computer Society*, 131–134.

[3] Peng J, Zhang X, Lei Z, Zhang B, Zhang W, an Li Q.[2009] Comparison of several cloud computing platforms, in Proceedings of the 2009 Second International Symposiumon Information Science and Engineering, ser. ISISE '09.Washington, DC, USA: *IEEE Computer Society*, pp. 23–27.

[4] Ristov S, Gusev M, and Kostoska M.[2012] Cloud computing security in business information systems,*International Jour-nal of Network Security & Its Applications (IJNSA)*, 4(2): 75–93.

[5] Eucalyptus. Eucalyptus cloud. [Retrieved: March, 2013].[Online]. Available: http://www.eucalyptus.com/

[6] OpenNebula. Opennebula cloud software. [Retrieved: March,2013]. [Online]. Available: http://Opennebula.org

[7] Cordeiro TD, Damalio DB, NCVN et al.[2010]Mangs,Open source cloud computing platforms, in Proceedings of the 2010 Ninth
International Conference on Grid and Cloud Computing, ser. GCC '10. Washington, DC, USA: *IEEEComputer Society*, 366–371.

[8] CSA. Cloud security alliance," [Retrieved: March, 2013]. [Online]. Available: http://cloudsecurityalliance.org/

[9] ISO/IEC, "ISO/IEC 27001:2005, Information Security Man-agement Systems - Requirements," [Retrieved: March, 2013]. [Online]. Available: http://www.iso.org/iso/iso catalogue cataloguetc/catalogue detail.htm?csnumber=42103

[10] Ristov S, Gusev M, and Kostoska M.[2012] A new methodology for security evaluation in cloud computing," in MIPRO 2012 Proc. of the 35th Int. Convention, *IEEE ConferencePublications*, 2012, pp. 1808–1813.

[11] ISO/IEC, WDTS 27017, Guidelines on infor-mation security controls for the use of cloudcomputing service Retieved: Mar 2013,Available:http://www.iso.org/iso/home/store/cataloguetc/cataloguedetail.htm?csnumber=43757

[12] CloudStack. Cloudstack opens source cloud comput- ing. [Retrieved: March, 2013].[Online]. Available: http://cloudstack.org

[13] Ristov S, Gusev M, and Kostoska M.[2012] Security assessment ofopenstack open source cloud solution, in Proceedings of the 7th South East European Doctoral Student Conference (DSC2012), pp. 577–587.

[14] Http:ftp://ftp.software.ibm.com/software/iea/content/com.ibm.iea.zos/zos/1.13/Security/zOS_V1R13_SSL_ECC-Support-for-TLS.pdf

[15] https-vs-http-website-ssl-tls-encryption-ranking-seo-secure-connection/

[16] https:// Transport_Layer_Security#keyexchange-table

**DISCLAIMER: *This published version is uncorrected proof; plagiarisms and references are not checked by IIOABJ; the article is published as provided by author and checked/reviewed by guest editor.*