IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Issue-4 E-ISSN: 2347-2693

Implementation of Multiple layer security of Cloud server

Neetu Rani[1*], Sandeep Dalal[2]

[1]DCSA, Maharshi Dayanand university, India
[2]DCSA, Maharshi Dayanand University, India

**Corresponding Author: agneetuchoudhary@gmail.com*

Available online at: www.ijcseonline.org

Received: 10/Mar/2018, Revised: 17/Mar/2018, Accepted: 29/Mar/2018, Published: 30/Apr/2018

***Abstract*:** Cloud computing is allowing business to focus on core businesses in spite of pay additional amount. Cloud environment has been considered as a model that is enabling access to a shared pool of configurable remote resources on demand. In this research the multi layer security for the cloud servers have been provided. It has been found that cloud services are offering flexible & scalable services. But there is always issue of security during information transmission from centrally located server storage to another location. Thus there is need to enhance the security of traditional cloud systems. Here in this paper need of cloud computing has been discussed along with its limitations. Focus of research is to provide security to cloud server, Security issue with existing system, cloud Server Model and programming module to perform encryption decryption and IP verification has been discussed.

Keyword: - Cloud Computing, Transferred, Storage

I. INTRODUCTION

Cloud computing[1] is internet based computing that is providing shared computer processing resources & devices on demand[2] & information to personal computer. It is considered as a model to enable access to a shared pool of configurable computing resources on demand. It could be released in smallest management system power. It has been some storage solutions are particular users & business within different storage capabilities & process in sequence in either owned in private or some party information centers which might be situated distant from user ranging distant from across a city to across world. It is depending on resources in order to received compatibility of scale, which is c comparable to usefulness over power network [3]. Promote proclaim that cloud computing permits more group to ignore up-front infrastructural price. This allows business to concentrate on core businesses in spite of spending money & time on personal computer infrastructure.

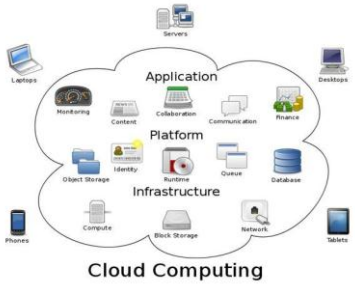

Fig 1 Cloud Computing

Need of Cloud computing

Cloud computing is required [4] due to following reasons:

1. It provides high availability.
2. It saves cost of hardware resources.
3. It saves cost of application software.
4. It reduces the maintenance cost at client end.
5. 24 hour online cloud allows multiple cloudlets to perform complex tasks.
6. Cloud environment provide high availability.

Limitation of Cloud computing

However cloud environment is providing lot of benefits but it has still several limitations. Some of them are stated below:

1. Cloud computing is dependent of Internet.
2. Cloud setup requires highly qualified[5] manpower.
3. The cost of cloud hardware is also limitation of cloud computing.
4. The threat of data loss is one of the major limitations.
5. The security threats at different layer also act as hurdle in frequent use of cloud.

II. SECURITY ISSUES IN CLOUD COMPUTING

There is lot of security [6] threat to the cloud environment. The cloud environment is based on network. Existing

researches are unable to tackle the problem of security issues in cloud computing [7]. There are several threats at different layers.

1. **Physical Layer attack [8]** suggests physical action such as disrupting source of power source, modification of interface pins, or the cable cutting. Tampering with fuse box could cause a interruption of service.
2. **Data Layer attack [9]** suggests the modification of ARP cache by Attackers so that computers associate the wrong MAC Address with the IP.
3. **Network layer attack** suggests attacker would use the proxy server as it would make tracking harder. Routers that are running old software versions could be relatively easy to attack.
4. **Transport layer attack** suggests attacker to perform **p**ort scanning of network in order to attack. NMAP is commonly used port scanner.
5. **Session layer attack** suggests TCP session hijacking, when a hacker takes over a TCP session among two machines.
6. **Presentation layer attack considers** Unicode Vulnerability. Originally Unicode has been designed to be universal, unique as well as uniform.
7. **Application layer attack:** The application layer[10] is hardest to defend. Vulnerabilities encountered here often rely on complex user input scenarios that are hard to define within an intrusion detection signature. Application layer is must be easy to use over Port 80 or Port 443. The application layer in OSI model is closest to end user. It means both OSI application layer and user interact directly within software application. Transmission Control Protocol or internet protocol specifications described a lot of applications that were at top of protocol stack.

DATA SECURITY ON CLOUD

Third party provides information & infrastructure management in cloud computing so security of cloud is biggest concern [11]. There is a risk in providing sensitive information to cloud service provider. Any security breach could result in customer or business loss so venders provide protection to accounts. Customer cannot switch from one cloud service provider to another quickly so he is dependent on cloud service provider for service.

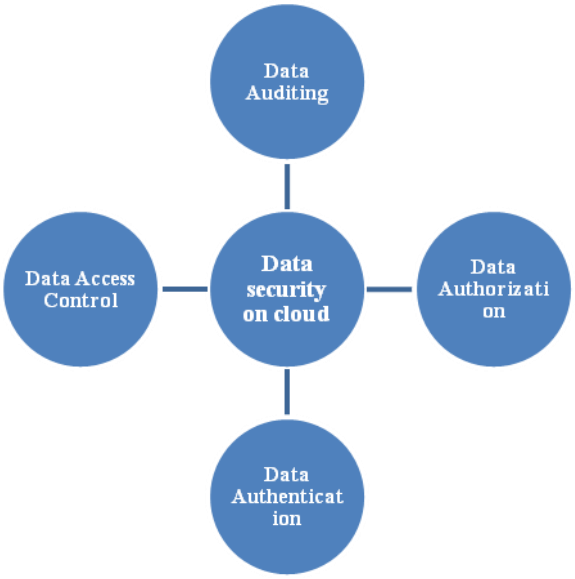

Fig 2 Data Security on cloud

Customer management interface is usually accessible on network in case of various public cloud service providers.

III. PROPOSED WORK

Here we discuss client server based model, Socket programming and enhanced AES encryption mechanism. Socket programming methodology consists of port and IP address.

Client Server based Model

Proposed work is based on client server model [15] where server implements first & waits to receive information client implements second & then sends first network data packet to server. Server authenticate user & user authenticate server generating a very strong session key using their shared password over an insecure channel by using symmetric cipher.

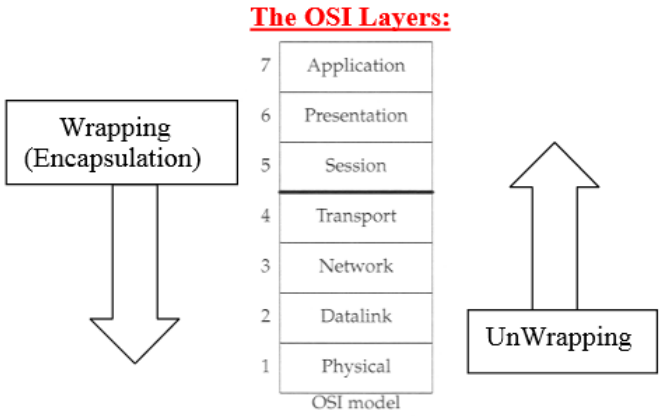

Fig 3 OSI Model

IP ADDRESS: The transmission of data would be performed on authorized IP addresses.
PORT: User defined ports would be used to establish the connection. This would reduce the probability of port scanning attack at transport layer. The transmission [16] would be made only when both client and server port are open. This would reduce the chances of session hijacking.
ENCRYPTION: Cryptography [16] of data would provide data security to the cloud.
Proposed model would create a separate layer for information transmission & hacker [15] would not be capable to access information on wireless network without application layer required on client.

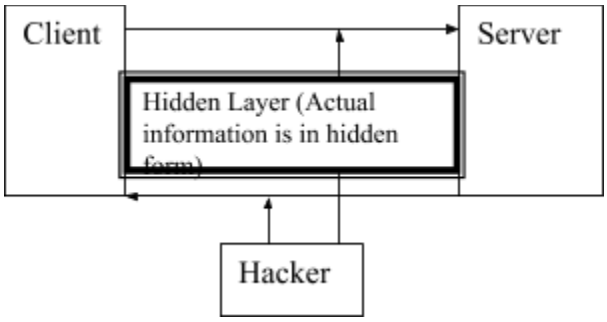

Fig 4 Proposed Model

Due to limitation of existing security mechanisms there was need to develop a new security system. The chance for decryption without authentication should get reduced. We need to implement IP filter based security in order to prevent attacker from different network. Here we would also reduce size of packet during transmission using replacement policy. We would enhance Advanced Encryption standard by introducing multilayer security. ***The proposed model offers following benefits as compare to traditional work.***

1. Proposed work considers the existing threats and opts to eliminate them.
2. User defined port mechanism would reduce the probability of port scanning attack.
3. Proposed work reduces the chances of session hijacking.
4. Proposed work would make use for more secure cryptography mechanisms in order to secure the information sharing over cloud
5. Information could be shared on authorized IP addresses.

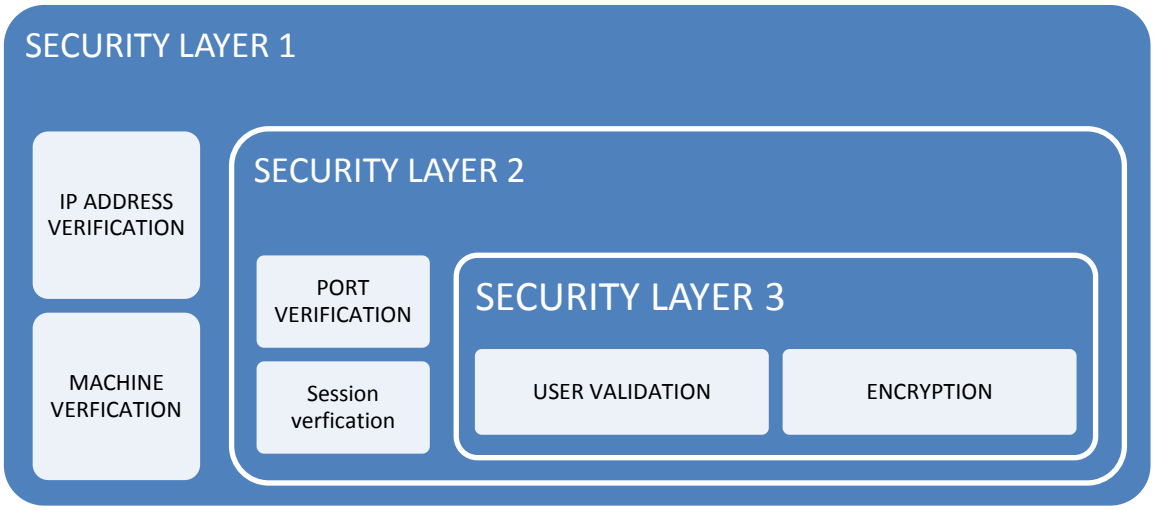

Fig. 5 Triple Layer Security

PROPOSED ALGORITHM

1. **At first stage IP address and Machine address is confirmed to reject unauthenticated transmission of packets from server to client.**
2. **In second level the port address of sender and receiver is confirmed to allow transmission.**
3. **The session is confirmed if session is invalid then data cannot be transmitted**
4. **If packet arrives at this stage then user is authenticated.**
5. **If packet is eligible for transfer then enhanced AES ENCRYPTION module works.**

i. TAKE PLAIN TEXT (256 bits)
ii. APPLY ROUND KEY and set counter=1
iii. if counter is less then 9
a) Process sub byte.

b) Perform Shift row
c) Mix columns
d) counter=counter+1;

iv. other wise
a) process subbytes
b) shift the rows
c) Apply round key

v. Cipher text would be generated (256 bits)

6. Perform the data Transmission
7. At receiving end the ip address and machine address is confirmed.
8. The port address and session is checked.
9. The user is authenticated here.
10. Perform the decryption of data at receiver end.

i. TAKE CIPHER TEXT (256 bits)
ii. APPLY ROUND KEY and set counter=1
iii. if counter is less then 9
a)Process Inverse shift row.
b)Perform inverse sub byte
c)Inverse Mix columns
d)counter=counter+1;
iv. other wise
a)Inverse shift rows
b)Inverse sub byte
c)Apply round key
v. Plain text would be generated (256 bits)

IV. IMPLEMENTATION

1 MULTILAYER SECURITY OF DATA ON CLOUD SERVER

There are lot of resources such as remote personal computer, cloud server & cloud storage connected to our systems. There is requirement of multiple layer security. So that user could not transfer information on unauthentic system.Following window represents systems connected to cloud server such as remote personal computer s & remote cloud storage.

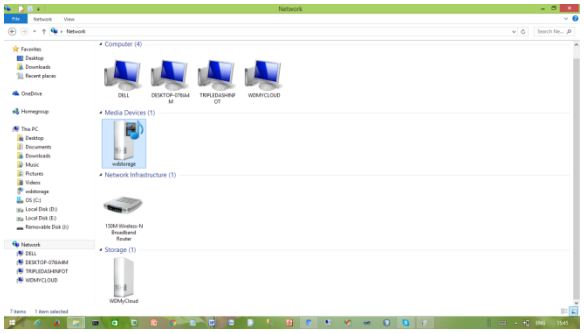

Fig 5 cloud server

Code for Base64

```
import java.io.*;

public class Base64
{
   public static String enc(byte[] dt1)
   {
      char[] aaaaa = {

         'A','B','C','D','E','F','G','H','I','J','K','L','M','N','O','P','Q'
W','X','Y','Z','a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r',
's','t','u','v','w','x','y','z','0','1','2','3','4','5','6','7','8','9','+','/' };

      StringBuilder buffer = new StringBuilder();
      int xpad = 0;
      for (int i = 0; i < dt1.length; i =i+ 3) {
 int b = ((dt1[i] & 0xFF) << 16) & 0xFFFFFF;
         if (i + 1 < dt1.length) {
            b |= (dt1[i+1] & 0xFF) << 8;
         } else {
           xpad++;
         }
         if (i + 2 < dt1.length) {
            b |= (data[i+2] & 0xFF);
         } else {
            xpad++;
         }

         for (int j = 0; j < 4 - xpad; j++) {
            int c = (b & 0xFC0000) >> 18;
            buffer.append(aaaaa[c]);
            b <<= 6;
         }
      }
      for (int j = 0; j < xpad; j++) {
         buffer.append("=");
      }

      return buffer.toString();
   }
```

Code to encrypt information using AES

Aes encryption

```
public class AES
{

         k1 = shsh.digest(k1);
         k1 = Arrays.copyOf(k1, 16);

         secretKey = new SecretKeySpec(k1, "AES");

               } catch (Exception e) {
               }
   }
```


IP BASED AUTHENTICATION

Every system has unique IP address that could be checked using ping command.

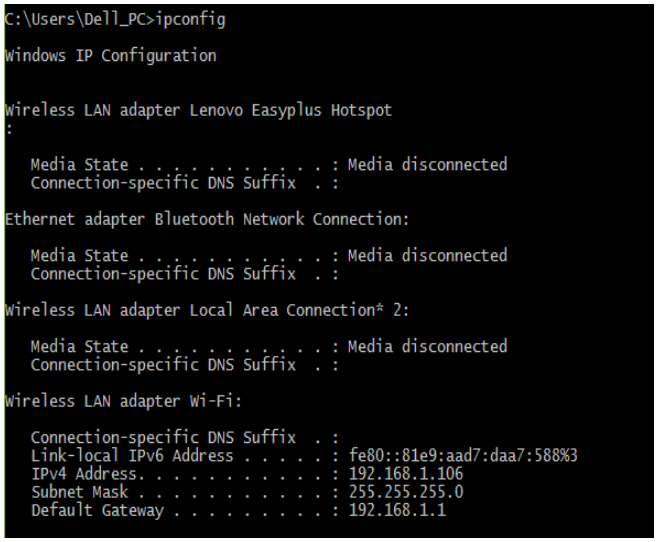

Fig 6 has unique IP

Generally user can set IP address of system manually or dynamically.

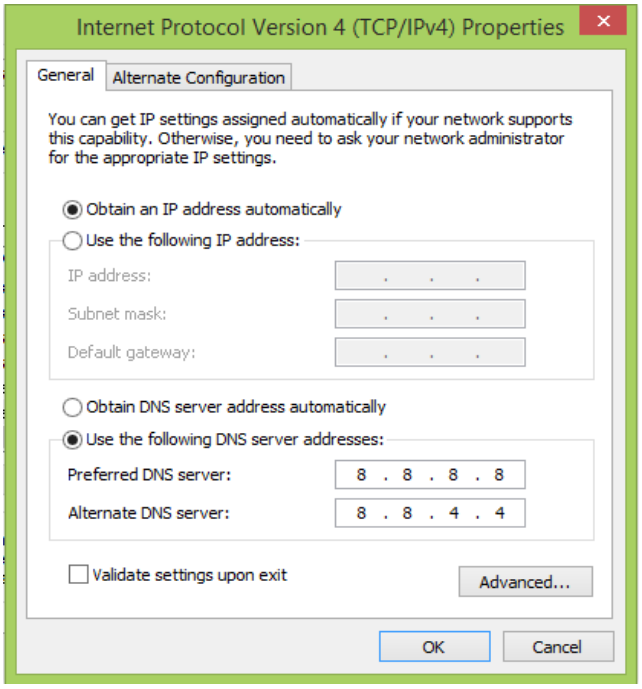

Fig 7 IP TABLE

Here we have given a IP TABLE that would authenticate IP address of client. This table assures list of valid IP address of client who are eligible to decrypt data.

iptable

IP	STATUS	Add New Field
1.0.0.1	1	
126.0.0.1	0	
127.0.0.1	0	
128.0.0.1	1	
*		

Following Code would authenticated IP Address

In this code it is checked from database whether IP address is valid or not

```
static int  isvalidip(String dd)
{
int flag=0;
try
        {
        Class.forName("sun.jdbc.odbc.JdbcOdbcDriver");
Connection
cn=DriverManager.getConnection("jdbc:odbc:edu","","");
        Statement st=cn.createStatement();
       ResultSet  rs=st.executeQuery("select  count(*)  from
iptable where ip like '" + dd + "' &   status =1" );
                while(rs.next())
        {
        flag=
Integer.parseInt(rs.getString(1));                }       }
```

V. CONCLUSION

Proposed work has considered the existing threats and tried to eliminate them. The user defined port which has been used above 1024. This is because 0 to 1023 ports are reserved. This mechanism would reduce the probability of port scanning attack. In proposed work chances of session hijacking has been reduced. There was security of data at application layer only in case of traditional work. Present work has been provided security to the packet. Chance for decryption without authentication should get reduced. There is need to implement IP filter based security in order to prevent attacker from different network would enhance Advanced Encryption standard by introducing multilayer security. This work has made use of more secure cryptography mechanisms thus it is providing better security approach. IP validation has also played significant role in enhancing the security of cloud network.

Reference

[1]. Peter mill & Tim grance, "The NIST Definition of Cloud Computing", 2011, National Institute of Standards & Technology ,Gaitherbsburg,MD 20899-8930, NIST Special Publication 800-145.

[2]. Ellen Messmer, "New security demands arising for virtualization, cloud computing", 2011, security-demands-arising-for-virtualization—cloud computing.html
[3]. .Sumedha Kaushik & Ankur Singhal, "Network Security Using Cryptographic Techniques" 2012, volume 2, Issue 12.
[4]. Charles Miers, Fernando Redigolo & Marcos Simplicio, A quantitative analysis of current security concerns & solutions for cloud computing , 2012, Journal of Cloud Computing: Advances, Systems & Applications electronic version of this article is
[5]. Rabi Prasad Padhay, "An Enterprise Cloud Model for Optimizing IT Infrastructure", 2012, International Journal of Cloud Computing & Services Science (IJ-CLOSER) Vol.1,
[6]. Nelson Gonzalez, et. al. , "A quantitative analysis of current security concerns & solutions for cloud computing ", 2012, Journal of Cloud Computing: Advances, Systems & Applications doi:10.1186/2192-113X-1-11The electronic version of this article is complete one & could be found online
[7]. .CSA "Security Guidance for Critical Areas of Focus in Cloud Computing", (2009), Tech. rep., Cloud Security Alliance..
[8]. Yet-Chun Hu, Ahmed M. Al Naamany, "Attacks within Wireless Networks" International Journal of Engineering Science & Technology (IJEST) ISSN : 0975-5462 Vol. 3 No. 4 April 2006, pp. 268-279
[9]. C. Sanchez-Avila, "analyzed structure & design" International Journal of Engineering Science & Technology Vol. 8 No 2007, , pp. 350–355,
[10]. Soufiene Djahel, "Defending Against Packet Dropping Attack In Vehicular Ad Hoc Networks Security & Communication Networks Security Comm." Networks 00: 1–13 (2008), pp. 510-520
[11]. Susan, Darshan Lal, "Destruction Security field is a new & fast moving career" International Journal of Advance Research in Computer Science & Management Studies on 2008, , pp. 345–355,
[12]. Michigan dear born, "security & privacy in emerging wireless networks" International Journal of Production Economics, Vol.112, pp. 510-520 (2010)
[13]. Shari Mohammadi, Reza Ibrahim Atani, Hussein Jadidoleslamy (2011) "A Comparison of Link Layer Attacks on Wireless Sensor Networks", Journal of Information Security, 2011, PP. 448-460,
[14]. Mahendra Kumar Mishra , "A Trustful Routing Protocol for Ad-hoc Network Global Journal of Computer Science & Technology" Volume 11 Issue 8 Version 1.0 might 2011, PP. 520-545
[15]. B.Maheshwari, Assistant Professor, Dept. of Informatics,(2012) "Secure Key Agreement And Authentication Protocols" International Journal of Computer Science & Engineering Survey (IJCSES) Vol.3, No.1, February 2012, PP. 437-444
[16]. Sumedha Kaushik, "Network Security Using Cryptographic Techniques" Journal of Civil Engineering & Management, Vol.17, No.3, pp. 437-444, 2012.
[17]. Wajeb Gharibi & Maha Shaabi (2012) Cyber threats in social networking websites, International Journal of Distributed & Parallel Systems (IJDPS) Vol.3, No.1, January 2012, PP 489-513
[18]. Jason V. Chang," computer hacking making", 2012 Journal of Zhejiang University-SCIENCE C (Computers & Electronics), pp. 530-540
[19]. Tongguang Ni, Xiaoqing Gu, Hongyuan Wang, & Yu Li (2013) Real-Time Detection of Application-Layer DDoS Attack Using Time Series Analysis, Journal of Control Science & Engineering Volume 2013, pp. 2287–3229
[20]. Dr. Mazin Sameer Al-Hakeem, " Development of Fast Reliable Secure File Transfer Protocol ", Journal of Zhejiang University-SCIENCE C (Computers & Electronics), 2013 15(7):pp 489-513
[21]. Hong-Ning Dai, QiuWang, Dong Li, & Raymond Chi-Wing Wong (2013) On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas, International Journal of Distributed Sensor Networks Volume 2013
[22]. P. Narendra Reddy, "Routing Attacks In Mobile Ad Hoc Networks International Journal of Computer Science & Mobile Computing" Vol. 2, Issue. 5, might 2013, PP. 612-625
[23]. Mukesh Barapatre, Prof. Vikrant Chole, Prof. L. Patil (2013) A Review on Spoofing Attack Detection in Wireless Adhoc Network, International Journal of Emerging Trends & Technology in Computer Science, Volume 2, Issue 6, November – December 2013, PP. 877-886
[24]. Sharad Pratap Singh, " security configuration & performance analysis of ftp server", intelligent Computing, Networking, & Informatics Advances in Intelligent Systems & Computing Vol. 243, 2014, pp 45-56
[25]. Sangeeta Yadav (2014) "Hybrid TCP/IP & UDP: A Review Article" International Journal of Advanced Research in Computer Science & Software Engineering, Volume 4, Issue 5, May 2014, PP. 56-68
[26]. Zainab Hassan.: "Performance Analysis of Dynamic Wireless Sensor Networks using Linguistic Fuzzy" Advanced Engineering Informatics, sVol.27, No.1, pp. 108-119, 2014
[27]. Amandeep Kaur, Dr. Amardeep Singh (2014) A Review on Security Attacks in Mobile Ad-hoc Networks, International Journal of Science & Research, Volume 3 Issue 5, May 2014, PP. 112-125

