© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 06 Issue: 02 | May-June 2015

Enhancement of Cloud Server Security by Customized Encryption Technology

*Nitu Singh, S.B.I.E.T, nitusingh74@gmail.com
**Matish Garg, Assistant Professor in cse department, S.B.I.E.T

Abstract: Cloud computing proposes new ways to provide services. These pioneering technical and pricing opportunities bring changes in the way business operated. Cloud computing is a new label to a traditional idea. Cloud computing is a set of resources provided by cloud service provider through internet. Lack of security is the only barrier in wide adoption of cloud computing. The rapid growth of cloud computing has brought many security challenges for users. Cloud computing offers many benefits, but it also is vulnerable to threats.

[I] Introduction

Cloud computing is the unique computing technology. Cloud computing is group of resources that are being allocated on demand. Cloud computing proposes new ways to provide services. These pioneering technical and pricing opportunities bring changes in the way business operated. Cloud computing is a new label to a traditional idea. Cloud computing is a set of resources provided by cloud service provider through internet. Cloud services are distributed from data centers sited all over the world. Cloud computing allows users to use the virtual resources. Cloud computing grabbed the spotlight in few years. Example of cloud services are Google Engine, Office 365, Oracle Cloud. As the cloud computing is growing rapidly it also leads to severe security concerns.

[II]Cloud Computing Model

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. However, cloud computing technology challenges many traditional approaches to datacenter and enterprise application design and management. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered as the characteristics of this innovative deployment model can differ widely from those of traditional architectures. An alternative perspective on the topic of cloud security is that this is but another, although quite broad, case of "applied security" and that similar security principles that apply in shared multi-user mainframe security models apply with cloud security. It is the very nature of cloud computing-based services, private or public, that promote external management of provided services.

Cloud Models are as follow

- Delivery Models
  - SaaS
  - PaaS
  - IaaS
- Deployment Models
  - Private cloud
  - Community cloud
  - Public cloud
  - Hybrid cloud

Private Cloud

Private cloud is the phrase used to describe a cloud computing platform that is implemented within the corporate firewall, under the control of the IT department. A private cloud is designed to offer the same features and benefits of public cloud systems, but removes a number of objections to the cloud computing model including control over enterprise and customer data, worries about security, and issues connected to regulatory compliance.

Public Cloud

A *public cloud* is one based on the standard *cloud* computing model, in which a service provider makes resources, such as applications and storage, available to the general *public* over the Internet. *Public cloud* services may be free or offered on a pay-per-usage model.

Hybrid Cloud

A hybrid cloud is a cloud computing environment in which an organization provides and manages some resources in-house and has others provided externally. For example, an organization might use a public cloud service, such as Amazon Simple Storage Service (Amazon S3) for archived data but continue to maintain in-house storage for operational customer data.

The hybrid approach allows a business to take advantage of the scalability and cost-effectiveness that a public cloud computing environment offers without exposing mission-critical applications and data to third-party vulnerabilities. This type of hybrid cloud is also referred to as hybrid IT.

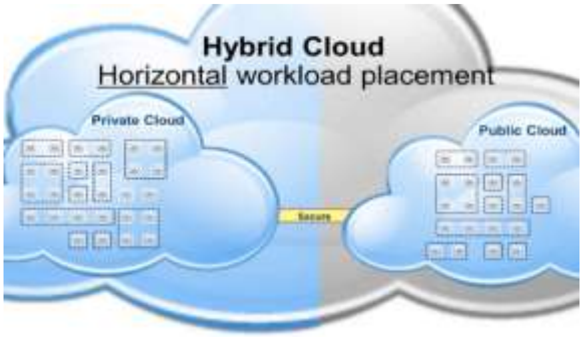


Fig.1 Hybrid Cloud

[III]Challenges

Lack of security is the only barrier in wide adoption of cloud computing. The rapid growth of cloud computing has brought many security challenges for users. Cloud computing offers many benefits, but it also is vulnerable to threats. One of the main threat exist today is the problem of unauthorized users or entities. For avoiding this problem the new technique is developed in this cloud computing is that data owners may share their outsourced data with a large number of users, who might want to only retrieve certain specific data files they are interested in during a given session.

[IV]Proposed Implementation

Proposed Cryptrography

Encryption Steps:-

- Encryption of plaintext that is to be send by the sender using encryption from secret picture which is actually sender's private key and thus generating cipher text using DES.
- Further, it will carry out the processon secret picture by the use of covered picture which is receiver's public key and thus encrypting with Rivers Shamir Adleman algorithm i.e. RSA.
- A digital envelope is sent to receiver having cipher text and picture so encrypted.

Decryption Steps:-

The Decryption of the message received from sender's side will occour as follow:

- Digital envelope will reach receiver's side.
- Digital envelope will be opened to get encrypted picture and decrypt using its own private key with RSA algorithm and receiver get secret picture.
- Cipher text will be changed using planet extusing secret picture applying DES.
- Thus receiver will get the plain text.

Proposed Socket implementation after proposed Cryptography

Here we will create our server and client communication protocol using own port using socket programming.

1. **First step is to create server side port using following algorithm**
   - Create ServerSocket object using our own port 6666.
   - Accept client request using Server socket object.
   - Receive data from client in form of input data stream object.
   - Convert data stream object to string
   - Input data stream is in form of cipher data decrypted using proposed algorithem.
   - Close the Connection
2. **Second step is to create Client side interface to connect to server.**

- Create ServerSocket object using our own port 6666 to connect to server
- Encrypt data before sending.

- Send data using data output stream object.
- Clean output buffer.
- Close the connection.

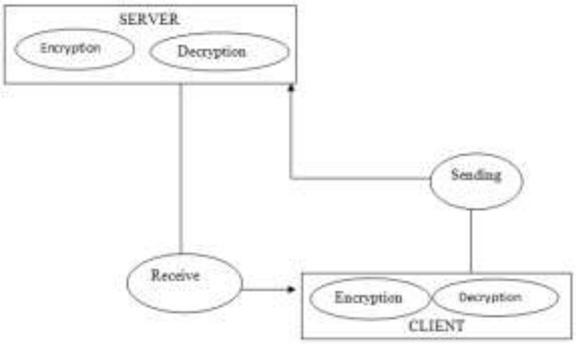


Fig. 2

Socket Programming

Let's see a simple of socket programming in which client sends a text and server receives it.

File: MyServer.java

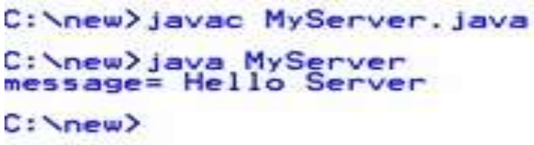
```
import java.io.*;
import java.net.*;
public class MyServer {
public static void main(String[] args){
try{
ServerSocket ss=new ServerSocket(6666);
Socket s=ss.accept();//establishes connection
DataInputStream dis=new DataInputStream(s.getInput
Stream());
String  str=(String)dis.readUTF();
System.out.println("message= "+str);
ss.close();
}catch(Exception e){System.out.println(e);}
}
}
```

File: MyClient.java

```
import java.io.*;
import java.net.*;
public class MyClient
{
public static void main(String[] args)
{
try
{
Socket s=new Socket("localhost",6666);  DataOutputS
tream dout=new DataOutputStream(s.getOutputStrea
m());
dout.writeUTF("Hello Server");
dout.flush();
dout.close();
s.close();
}
catch(Exception e)
{
System.out.println(e);
}
}

}
```

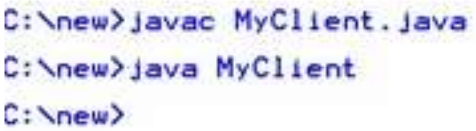
To execute this program open two command prompts and execute each program at each command prompt as displayed in the below figure.



```
C:\new>javac MyServer.java
C:\new>java MyServer
message= Hello Server
C:\new>
```

Fig 3. Execution of server

After running the client application, a message will be displayed on the server console.



```
C:\new>javac MyClient.java
C:\new>java MyClient
C:\new>
```

Fig 4. Execution of Client

[V] Future Scope and Conclusion

We have enhanced the security by enhancing encryption algorithm.

Here we have also defined our own ports for server and client and defined new rules for encryption and decryption this will definitely improve the security mechanism in Cloud computing environment.

References

[1] David Pointcheval, Olivier Blazy, New Smooth Projective Hash Functions and One-Round Authenticated Key Exchange(18_22 august 2013, Santa Barbara, California, USA), Springer-Verlag, LNCS 8042, pages 449_475.

[2] David Pointcheval, Olivier Blazy, Effcient UC-Secure Authenticated Key-Exchange for Algebraic Languages(26 February - 1 March 2013, Nara, Japan)), 16th International Conference on Practice and Theory in Public-Key Cryptography (PKC '13)Springer-Verlag, Kaoru Kurosawa Ed., Springer-Verlag, 2013.

[3] David Pointcheval, Password-based Authenticated Key Exchange. (21-23 may 2012, Darmstadt, Germany)Springer-Verlag, LNCS 7293, pages 390-397.

[4] David Pointcheval, Michel Abdalla, Contributory Password-Authenticated Group Key Exchange with Join Capability, (February 14-18, 2011, San Francisco, CA, USA), A. Kiayias Ed. Springer-Verlag, LNCS 6558, pages 142-160.

[5] David Pointcheval, Xavier Boyen, Strong Cryptography from Weak Secrets, (3 – 6 may 2010, Stellenbosch, South Africa), D. Bernstein and T. Lange Eds., Springer-Verlag, LNCS 6055, pages 297–315.

[6] David Pointcheval, Michel Abdalla, Flexible Group Key Exchange with On-Demand Computation of Subgroup Keys, (3-6 May 2010, Stellenbosch, South Africa)), D. Bernstein and T. Lange Eds., Springer-Verlag, LNCS 6055, pages 351-368.

[7] David Pointcheval, Michel Abdalla, Distributed Public-Key Cryptography from Weak Secrets, (18_20 march 2009, Irvine, CA, USA), S. Jarecki and G. Tsudik Eds. Springer-Verlag, LNCS 5443, pages 139_159.

[8] David Pointcheval, Michel Abdalla, Password-Authenticated Group Key Agreement with Adaptive Security and Contributiveness, (21 – 25 june 2009, Gammarth, Tunisia) B. Preneel Ed., Springer-Verlag, LNCS 5580, pages 254–271.

[9] Rafael Álvarez, Leandro Tortosa, Analysis and design of a secure key exchange scheme, Information Sciences 179 (2009) , Elsevier

[10] David Pointcheval, Michel Abdalla, Anonymous and Transparent Gateway-based Password-Authenticated Key Exchange , December 2–4, 2008, Hong-Kong, China – M. Franklin, L. Hui and D. Wong Eds. Springer-Verlag, LNCS 5339, pages 133–148.

[11] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval, Provably-Secure Authenticated Group Diffie-Hellman Key Exchange, ACM Transactions on Information and System Security, Vol. 10, No. 3. August 2007.

[12] Kumar Mangipudi, Rajendra Katti, A Secure Identification and Key agreement protocol with user Anonymity (SIKA), journal homepage: www.elsevier.com/locate/cose, Computers & security 25(2006) 420 – 425.

[13] Chin-Chen Chang, Jung-San Lee, An anonymous voting mechanism based on the key exchange protocol, journal homepage: www.elsevier.com/locate/cose, Computers & security 25(2006) 307– 314.

[14] Tseng, Y.M., 2005, Weakness in simple authenticated key agreement scheme, Electronics. Letters 36 (1) pp. 48–49.