UGC APPROVED JOURNAL - 47746

© INNOVATIVE RESEARCH THOUGHTS | Refereed | Peer Reviewed | Indexed

ISSN : 2454 – 308X | Volume : 03 , Issue : 10 | October – December 2017

Enhancement of Cloud Server Security by Customized Encryption

Pooja Bansal

Email id poojasinghal273@gmail.com

Abstract:

Using cloud computing, new methods of delivering services may be explored. These cutting-edge technological and price possibilities alter the way business is conducted. The term cloud computing refers to an old concept given a new name. A cloud computing service is a collection of resources made available through the internet by a cloud provider. Cloud computing adoption has been stymied by a lack of security. "As cloud computing has grown, so has the number of security concerns for consumers. However, cloud computing has a number of advantages, as well as risks.

[I] Introduction

Unlike any other computer technique, cloud computing is unique. The term cloud computing refers to a set of resources that may be accessed at will. Using cloud computing, new methods of delivering services may be explored. These cutting-edge technological and price possibilities alter the way business is conducted. The term cloud computing refers to an old concept given a new name. A cloud computing service is a collection of resources made available through the internet by a cloud provider. Data centres located all around the globe host the cloud services. The virtual resources may be accessed using cloud computing. In the last several years, cloud computing has taken centre stage. These include Google Engine, Office 365, and Oracle's Cloud computing platform. The fast growth of cloud computing has led to serious security problems.

[II]Cloud Computing Model

To put it simply, cloud computing is a methodology for providing on-demand network access to a shared pool of customizable computing resources (such as network bandwidth and server resources) that can be quickly supplied and released with minimum administration effort or service provider engagement. There are numerous established ways to datacenter and business application design and administration that are being challenged by cloud computing technologies. In light of the unique features of this new deployment paradigm, classic protective measures are being re-evaluated for their efficacy and efficiency. Another way of looking at cloud security is to see it as just another example of applied security, comparable to the shared multi-user mainframe security models that apply similar security concepts. The very nature of cloud computing-based services, whether private or public, encourages external administration of the services that are offered..

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.

[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.

Security issues in Cloud

With growing cloud capabilities, security is becoming a major challenge in wide adoption of cloud. Can users fully trust cloud? Is their data safe on cloud? These questions are emerging with no reliable solutions yet. Moreover cloud is becoming particularly

attractive to cyber crooks. The cloud faces both internal and external security threats like media failures, software bugs, malware, administrator errors and malicious insiders.

Cloud services hold user's personal data and identity information such as photographs, calendars, address books, medical records, social security numbers, tax documents, financial transactions etc. These data if analyzed properly can tell every aspect of user's life. So significant safeguard is required to protect user's privacy. Consider banks and other financial institutions which process highly sensitive data, if they use cloud high degree of security is required for their data.

For hosted clouds, third party is responsible for storing and securing data. But are third parties trust worthy? Handing over sensitive data to other party is a serious concern. Trusting a third party requires taking the risk of assuming that the trusted third party will act as it is expected (which may not be true all the time). Data exposure risk stays from the level of one individual's data to the whole cloud level.

[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.

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.get
InputStream());

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);  DataOutp
utStream dout=new DataOutputStream(s.getOut
putStream());

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.

Fig 3. Execution of server

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

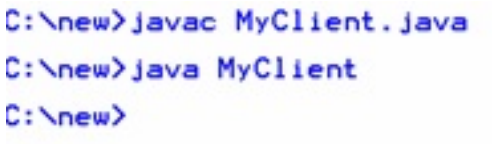

Fig 4. Execution of Client

[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.