ISSN: 0975-766X
CODEN: IJPTFI
Available Online through
www.ijptonline.com
Research Article

NOVEL CRYPTOGRAPHY ALGORITHM FOR SECURITY IN CLOUD COMPUTING

Dhinesh Babu L.D, Sharon Moses J, Shah Naitik B, Desai Nisarg M
School of Information Technology and Engineering, VIT University, Vellore - 632014, Tamil Nadu, India
Email: lddhineshbabu@gmail.com

Received on 25-10-2016 *Accepted on 02-11-2016*

Abstract

Cloud computing services, revolutionized the information technology to a greater extent. Also, evolution of cloud computing created many security issues especially data driven security issues. Since, all the cloud related services are carried out remotely using internet, building highly secured cloud computing environment for the secure transfer of information remains as trending research.In this work, the issues in securing the data are discussed elaborately then an enhanced cryptography based approach is formulated to safeguard the client data.

1. Introduction

Currently cloud computing services, evolved as one of the essential innovation of information technology [1]. Cloud offers all its services with minimal price. Instead of spending huge expense on buying hardware, people adopt to cloud computing where from deploying the service to maintaining it is taken care by cloud providers. Pay for what use payment method and the scalable nature of the cloud made many companies to adapt cloud computing services. Though many huge IT gaints like Amazon Web Services, Google, Microsoft and many more offer cloud services security remains as one of the primary concern [2]. Though many people adapted to cloud computing, they are in dilemma due to the security threats for the stored data in the cloud. Once the data is stored in the cloud, the exact location of the data will not be revealed to the client. Totaly authority over the data will be given to the cloud service provider [2]. Cloud service provider, may allow third party auditors to view the data. Also to ensure safety the data will be replicated and get stored in different servers residing in different geographical location [3]. Encrypting the data is the only best fit method to secure the data from security threats [4]. In this paper, various security threats faced by the data in the cloud are detailed then an enhanced cryptography method is designed to provide security to the data.

2. Cloud Computing Services

According to National Institute of Standards and Technology (NIST) Cloud computing is defined as the scalable model to easily access varied demanding computing resources like instances, storage servers, software application, servers and software services through connected network [5].

Cloud services classified into three, namely Software as Service (SaaS), Platform as Service (Paas) and Infrastructure as Service (IaaS)[5].

- IaaS: -HardwareTotal hardware infrastructure ranging from processors to storage is offered to customers through virtualization. Best example for Infrastructure as a service is Amazon Ec2.
- PaaS: - In Platform as a Service, users are provided with an instance. Using the instance they can develop and deploy any application. Heroku is one among the best example of PaaS.
- SaaS: -In Software as a service architecture provides software service to its client. Instead of purchasing software clients use cloud services to utilize the software and will pay for what they use. From maintaining to upgrading the software is done by cloud provider.

3. Cloud Deployment is carried out in the following ways

- Public Cloud: Public clouds are accessed by general public, no restrictions to the users who access the public cloud. Google’s Gmail is the one of the best public cloud.
- Private Cloud: - Cloud built and maintained by separate organization is the private cloud.
- Community Cloud: - Community cloud is built by the group of organizations who have common ideology.
- Hybrid Cloud: - Hybrid clouds are the mixture of public and private clouds. Two or more cloud architecture exist within one setup is the hybrid cloud

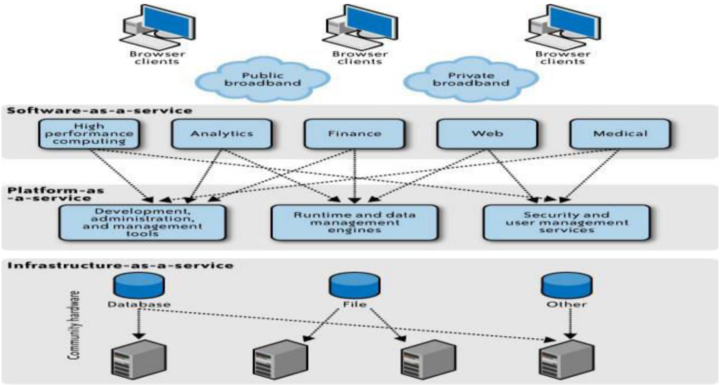


Figure-1 Cloud Service Architecture.

4. Data Security Concern in Cloud

Even though cloud offers scalable on demand services to the customer, Storing personal information in cloud always appears to be unsafe [2] [6]. In cloud, nobody knows where the data is getting stored. Even the cloud service providers do know the exact physical location of the data [7]. Once the user uploads the file into cloud storage, the file is replicated more than twice to ensure assured recoverability for the file. The file will get replicated and stored in different storage servers across the globe. In some geographical location, the information piracy law will abide the servers not to transmit or hold the file. If, a natural disaster affects the server than, it will be very hard to retrieve the stored file from the cloud storage. To ensure the integrity and nature of the file, cloud service provider will lend the auditing services to the third party auditors. Users, who stored their personal information, would not like the third party auditors or anyone to view their personal information. If a cloud service provider employee with authority to handle the file when turn into data thief, it will risk the user data. Competitors will try to access the critical information stored in cloud to overcome their business rivals. Since all the information is getting accumulated in the cloud, cloud storage servers became vulnerable to security attacks. Denial of service is another type of attack that creates security issue to the total cloud infrastructure. Some cloud service providers, encrypt the information before storing into storage servers. Though the files are getting encrypted, the encryption key is still remains the server [8]. When an intruder gains access to the key server, he may decrypt all the information in the server. In figure 2, existing technique of sending information from one end to other end is shown.

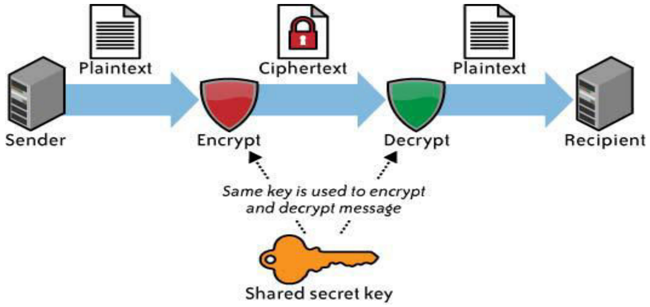


Figure-2: Existing Technique

5. Cryptography Based Technique

The trust remains the main factor between the user and the cloud service provider once trust on service provider is lost, user won't use the cloud based services. Safe guarding the data is the duty of both the user and the service provider. Some service providers provide the highest security to the paid services and very light weight security to the unpaid services. Initially service provider will educate the user about the security concerns of the storage. There should be a high level of transparency, so that user will trust the cloud service provider. In our proposed work the user data is compressed then encrypted based on ASCII value. Once encryption is done then using Diffie-Hellman algorithm the data is shared between user and the receiver.

- Steps Involved
  - Compress the Data
  - Based on ASCII Value of Compression Encrypt the Data
  - Share the encryption key using Diffie-Hellman key algorithm
  - At the end Decrypt Data using the encryption algorithm

- Diffie-HellmanAlgorithm.

```
1.  qPr = Prime Number;
2.  qPrRoot = primitive root of qPr where qPrRoot < qPr;
3.  ChoosepvtX1 where pvtX1<qPr;
4.  ComputepubY1=qPrRoot^ pvtX1 mod qPr;
5.  ChoosepvtX2 where pvtX2<qPr;
6.  Compute public YPub=As^XB modPr;
7.  key = ( pubY2)^ pvtX1 mod qPr;
8.  key = ( pubY1)^ pvtX2 mod qPr;
9.  For(ASCII=Compressed File)
    {
    DHAkey1[]=DHAkey1[] + Binary(ASCII);
    }
10. DHAkey[]=Transform DHAkey1[] to Cipher Format
```

6. Encryption Algorithm

The value that is generated from converting the compressed file is compared with 79,32 and 126. Based on the weightage, mathematical model is formulated then the final outcome is converted into binary value. Once the binary value is generated it is converted into cipher. The cipher and the outcome of Diffie-Hellman are summed up. The final outcome is converted into hexadecimal and transferred to the receiver..

```
1. data[]=get the Compressed message
2. ln= calculate length of the Compressed message
3. Construct For loop range (1:ln)
     ASCII=ASCII value of data[range];
     IF(ASCII==32)
         p=126;
     BinaryValue[]=∑(BinaryValue[],(Converted Binary Bit);
     Else IF (ASCII==126)
         p=32;
     Binary Value[]=∑(BinaryValue[],(Converted Binary Bit);
     Else If(ASCII>79 && ASCII!=126)
        m=ASCII-79;
        p=32+m;
     BinaryValue[]=∑(BinaryValue[],(Converted Binary Bit);
     Else If(ASCII<79 && ASCII!=32)
        m=79-Ascii;
        p=126-m;
     BinaryValue[]=∑(BinaryValue[],(Converted Binary Bit);
     Else
        p=79;
     BinaryValue[]=∑(BinaryValue[],(Converted Binary Bit);
4. CipherFinal[]=BinaryValue into CipherFinal;
5. CipherFinal[]=CipherFinal[]+ DHAkey[];
6. TransmitingMessage[]=CipherFinal[] into Cipher[] +Hexadecimal Code
```

7. Decryption Algorithm

The reverse operation to the encryption is done in the decryption process. The final transmitting message is converted into binary value. The receiver key from DHA Key and Sender DHA key is compared to verify whether the both key are same. If identical then they get deleted and the ciphered text is deciphered. As done in the encryption the ASCII value of compressed file is compared with 79,32 and 126. The mathematical model induced while encrypting is used again to convert the compressed file. Compressed file is decompressed to get the raw data.

```
a. TransmittingMessage[]=CipherFinal[]+Hexadecimal Code.
b. CipherFinal[]=Transform CipherFinal into DHAkey and BinaryValue
c. Check the DHAKey
          i. IF DHAKey of Sender and Receiver Identical
         ii. True
        iii. Then Delete the DHA Key and return the BinaryValue
d. BinaryValue[]=Binary Value+BinaryBit
e. Separate the Binary Value[] and the Binary Bit
f. For(range(Find Binary Bit where ASCII Value = Binary Bit))
   IF(ASCII==32)
     p=126;
   Decipher[]=Decipher[] + p to original character;
   Else IF(ASCII==126)
     p=126;
   Decipher[]=Decipher[] + p to original character;
   Else IF(ASCII>79 && ASCII!=126)
     m=126-ASCII;
     p=79-m;
Decipher[]=Decipher[] + p to original character;
   Else If(ASCII<79 && ASCII!=32)
```

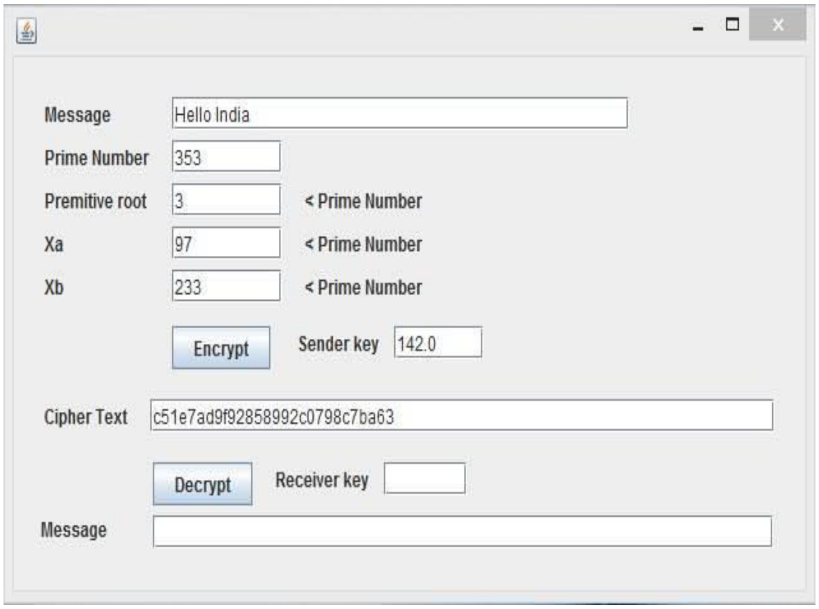
```
        m=ASCII-32;
        p=79+m;
      Decipher[]=Decipher[] + p to original character;
      Else
        p=79;
      Decipher[]=Decipher[] + p to original character;
```

g. Decompress the Deciphered data to get the raw Data.

8. Result

The proposed approach is successfully implemented and the results are depicted in the figure 3 and figure 4. Initially the raw data "Hello India” is typed into the console. The raw data is compressed and the prime value qPr is given as 363, pvtX1 and pvtX2 value as 97 and 233 and the qPrRoot value is given as 3.

When all this values are given, the algorithm computes and generates the DHA key as 142.0 and genreates the cipher text after encryption as c51e7ad9f92858992c0798c7ba63. After the conversion, the raw data is transferred from sender to receiver end. In figure 3 the conversion of raw data into Cipher is clearly depicted.



Message: Hello India

Prime Number: 353

Premitive root: 3 < Prime Number

Xa: 97 < Prime Number

Xb: 233 < Prime Number

Sender key: 142.0

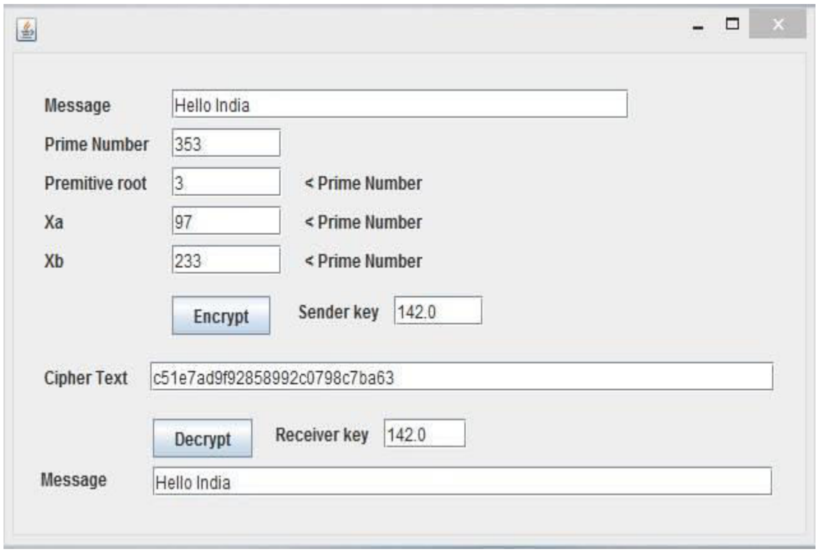
Cipher Text: c51e7ad9f92858992c0798c7ba63

Receiver key:

Message:

Figure-3: Encryption.

In figure 4, the computation of deciphering the encrypted raw text "Hello India" can be seen. When the receiver key is same as the sender key that is DHAKey, then the deciphering the ciphered text process gets started. Once the binary bit is separated from the ciphered text. After the compression process the original text can be deciphered totally into raw data.



Message: Hello India
Prime Number: 353
Premitive root: 3 < Prime Number
Xa: 97 < Prime Number
Xb: 233 < Prime Number
Sender key: 142.0
Cipher Text: c51e7ad9f92858992c0798c7ba63
Receiver key: 142.0
Message: Hello India

Figure-4: Decryption

9. Conclusion

Cloud computing with its meritoriousness nature pulls lot of general public and organizations to utilize its services. Though scalability and on demand service of cloud appears to be need of the hour, security in cloud remains as a threat. In the future, every house will have more than one terabytes of information. So the growing demand for cloud storage should be met out with proper security measures. The sensitive information that are getting stored in cloud storage needs additional security. On demand need of security, growing security attacks, data pirates, and denial of service attacks remains as the importance of new security paradigm to counter the security attacks. In the proposed work a simple yet powerful encryption algorithm, is introduced to protect the user information. In future, with the growing demand of security architecture, an enhanced cryptography based algorithm with light weight computation overhead will be proposed to secure files from the intruders.

References

1. E. D. Raj and L. D. Dhinesh Babu, “A firefly swarm approach for establishing new connections in social networks based on big data analytics,” *Int. J. Commun. Networks Distrib. Syst.*, vol. 15, no. 2–3, pp. 130–148, 2015.
2. L. D. Dhinesh Babu and P. Venkata Krishna, “Honey bee behavior inspired load balancing of tasks in cloud computing environments,” *Appl. Soft Comput. J.*, vol. 13, no. 5, pp. 2292–2303, 2013.
3. N. Wang, H. Liang, Y. Jia, S. Ge, Y. Xue, and Z. Wang, “Cloud computing research in the IS discipline: A citation/co-citation analysis,” *Decis. Support Syst.*, vol. 86, pp. 35–47, 2016.
4. D. Karaboga and C. Ozturk, “A novel clustering approach: Artificial Bee Colony (ABC) algorithm,” *Appl. Soft*

Comput. J., vol. 11, no. 1, pp. 652–657, 2011.

5. Z. Wei, G. Pierre, and C. H. Chi, "CloudTPS: Scalable transactions for web applications in the cloud," *IEEE Trans. Serv. Comput.*, vol. 5, no. 4, pp. 525–539, 2012.
6. E. Yadegaridehkordi, N. A. Iahad, and N. Ahmad, "User perceptions of the technology characteristics in a cloud-based collaborative learning environment: a qualitative study," *Int. J. Technol. Enhanc. Learn.*, vol. 7, no. 1, p. 75, 2015.
7. L. D. D. Babu and P. V. Krishna, "An execution environment oriented approach for scheduling dependent tasks of cloud computing workflows," *Int. J. Cloud Comput.*, vol. 3, no. 2, pp. 209–224, 2014.
8. "Available Online through An Optimal Iot Enabled Data Processing Approach For Effective Detection Of Remote Air Pollution issn : 0975-766x coden : ijptfi research article," vol. 8, no. 3, pp. 15496–15509, 2016.
9. H. Löhr, A. Sadeghi, and M. Winandy, "Securing the e-health cloud," *Proc. ACM Int. Conf. Heal. informatics - IHI '10*, p. 220, 2010.