FP- International Journal of Computer Science Research (IJCSR)
Volume 2, Issue 2, Pages143-147, June 2015

A Hybrid Chaotic Based Encryption Security in Cloud Computing

Jaspreet Mahal
Department of Computer Science
Chandigarh University
Punjab, India
Jaspreet.mahal@ymail.com

Sugandha Sharma
Department of Computer Science
Chandigarh University
Punjab, India
Sugandha.ss1@gmail.com

ABSTRACT

Cloud Computing is the latest technology in the field of distributed computing. Cloud computing has received heed seriousness in recent years but security issue is the one of the crucial inhibitor that decreasing the growth of cloud computing. Because of the data security issues, multiple organizations are unable to use the cloud sevices. To solve this problem, there have been several methods used by the researchers worldwide to increase the security. This paper proposed a hybrid algorithm that is the combination of RSA and the Advanced Encryption Standard algorithm with chaotic theory and it will be used to enhance the data security while storing the data on cloud. The RSA algorithm will be used to make authentication of each client and server more secured over the cloud and AES will be used for encryption/ decryption with random key.

General Terms

Security Issues, Encryption Algorithm, Service Models

Keywords

Cloud computing, Security issues, RSA, AES algorithm with Chaotic theory.

1. INTRODUCTION

Recently, Cloud computing is a new type of computing model for on demand network access to a shared pool of configurable computing resources that can be dynamically provisioned. The main motivation of the cloud computing is to provide scalable and low price on-demand computing infrastructures with fine quality of service levels. Many developers are struggling to make cloud-based applications secure for users. But it is not easy to provide real security with currently affordable technological abilities. Cloud computing is the combination of multiple cloud components interacting with each other about the various data they are carrying on too, thus helping the user to provide required data at faster rate. Cloud computing appears as a computational pattern as well as a architecture of distribution and the main objectives are to provide convenient, and secure data with all computing services seen as services broadcasted over the internet. Cloud computing integrates number of computing technologies Service Oriented Architecture (SOA), Web 2.0 and virtualization with reliance on the internet, and satisfy the computing requirements of the user with common business applications online with the help of web browsers.

Although, there are many benefits to acquiring cloud computing, there are also some significant bars to adoption. Security is the one of the most significant barriers to the adoption, stalked by issues regarding legal matters and privacy. Because a relatively new computing model of cloud computing defines the great deal of uncertainty about how the security is achieved at different levels and how security of applications are moved to cloud computing.

In recent years, development of internet has become fast[9]. The cost of storage and the power consumption of computer and hardware is increasing. Storage space in data center's can't fulfill the requirements of users that's why we need cloud computing to utilize the free resources of the computers and increase the economic productivity by enhancing the utilization rate.

1.1 Basically, cloud computing has three types of service models[7]

1.1.1 Software as a service (SaaS)

Software as a Service, the customer can use the applications that are already developed and the other users can use these services by on demand. SaaS is also called a Web based service.

1.1.2 Platform as a Service (PaaS)

To established a set of pre-packed products, platform as a service provide readymade environment to the users.

1.1.3 Infrastructure as a Service (IaaS)

Infrastructure as a Service provides high level of responsibility and the control over its configuration and utilization

.

2. SECURITY ISSUES

The major problems in cloud computing are data lock in, data confidentiality and data availability, software legal agreement, location transparency[8]. The main challenges that are faced by cloud computing are discussed below [5]:

2.1 Data loss:

After the deletion of data without any backup or the loss of encoded key make the cloud difficult to restore.

2.2 Location of data storage:

It is the one of the leading flexibilities for cloud computing, which is a security warning at the same time – without knowing the specific location of data storage.

2.3 Strong authentication

Authentication is one of the important factor that affects the cloud security. Without proper authentication, any malicious user can easily access the user's personal data stored on the cloud.

2.4 Multi-tenancy:

It means multiple users share the single instance of software application simultaneously. In this, pool of resources shared by tenants and having opposing goals. Security is the common concern related to customer perspective-is my data going to be secure or not? The chance of one user's data can be share by other user. Data isolation is necessary to overcome this issue.

2.5 Malicious insiders:

If a high authority person use the cloud services and he or she is using cloud servers to launch a DoS attacks then it will make the cloud computing unsecured[6].

3. EXISTING WORK

In cloud computing the main challenge is to provide the security of data and this data security is made by authentication, encryption and so on. So now, we discuss about some security issues and the solutions for this to enhance the security of cloud data.

Ashidh et al. [1] described the proposed Bi-Directional DNA encryption algorithm for encryption process. For key sharing, Diffi-Hellman key exchange algorithm was used. Firstly, user enter the message into Unicode plain text and then convert it into ASCII character set and then converted into Hexadecimal after that converts into binary code. Find the DNA coding using binary code from A,T,G and C that defined in this paper. Then find prime pair using PCR amplification and then amplified message is ready to send to the cloud. The decryption process is the reverse process of this. In last recent years security in cloud computing has become an important issue but encryption has come up as solution for providing network security to the data described by **prerna et al [2]**. It described the implementation of three encryption techniques like AES, DES and RSA algorithms. The block size used by AES 128 bits, DES used 64 bits and minimum 512 bits used by RSA. And compare the performance of encrypt techniques on the basis of their encryption time, decryption time. He or She has evaluated that the encryption and decryption time of AES was less as compared to DES and RSA and AES was much better algorithm than both of them. A proposed framework in which we can secure files through file encryption explained by **R G Suresh et al. [3]**. The file which is saved in the device will be encrypted using password based AES algorithm and the user can also read any files on the system by download the encrypted files. The four types of transformations: substitution, permutation, key-adding and mixing are used by AES to provide security. This approach was quite useful to prevent unauthorized person to access the file stored on cloud. **Debajyoti et al. [4]** explained the process of encrypted files upload to the cloud and the user can only access this data with proper authentication.

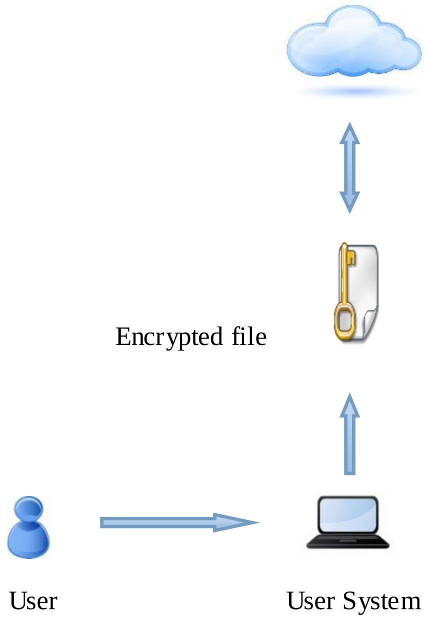

Figure 2. Represents file upload

AES algorithm is considered as a secured algorithm but there are some problems in the S-box and the key used. In this paper the main focus was on key used. To increase the security, the AES is simulated and tested with different chaotic variations[10].

4. PRESENT WORK

This section gives the problem formulation, objectives, methodology, design and implementation of the proposed work.

4.1 Problem Formulation

Cloud computing is the lately research area where researcher are trying to come up with a best solution for different issues over the cloud computing like security, data storage, resource allocation and many more. Here in this research work, we are focusing on the security aspect of the cloud. The thesis aims to solve a major problem with cloud computing related to providing security of data. Many cryptographic algorithms both symmetric and asymmetric are used for the security but neither the needs of the customer nor the need of system were satisfied. AES is a very famous encryption algorithm but has its limitations on grounds of simple power analysis (SPA), differential power analysis (DPA), higher order differential power analysis (HODPA) attacks.

4.2 Methodology

We have used the hybrid encryption algorithm using RSA and AES with chaotic theory. The RSA algorithm is used to make the authentication of each client and server more secured over the cloud. Earlier only client was authenticated by server, but we have proposed the method in which authentication is done by both client and server. The methodology includes two steps:

4.2.1 Authentication

It is the process of identifying a user. Earlier authentication was done from server side for client. Figure below shows the two way authentication from client and server. K_{PC}, K_{RC} pair of public and private key of client side and K_{PS}, K_{RS} are the pair of public and private key of server side. During the connection between server and client both will share their public key K_{PX} , (X is either server or client) with each other so that the further communication between the two will be secured, both will now communicate with each other after encrypting data with the each other's public key and decrypt their own private key, K_{RX} . At the client end username U , password P will be send along with the message R_{1C} which will be used to authenticate server. Rest of the steps is explained in the figure below.

4.2.2 Encryption

After successful completion of authentication between client and server, next step is for encrypting data before storing in the cloud. The encryption is done by cryptographic agent using Advance Encryption Standard algorithm. Whenever data is stored over cloud it will be encrypted using secret key asked at the time of uploading by the user / client. Basic architecture of cloud computing with authentication and encryption is shown in Figure 1.

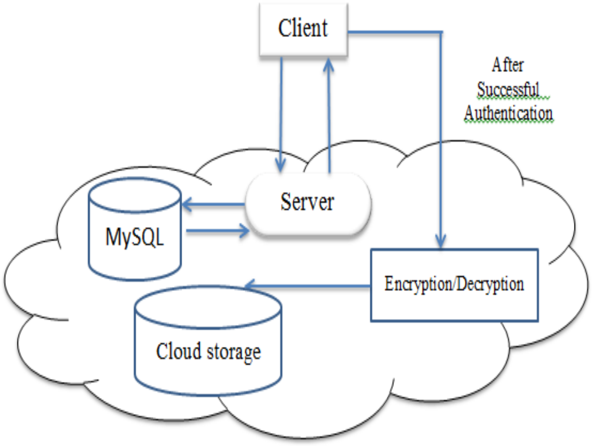

Figure 1 Basic architecture of cloud with encryption

4.2.3 Advanced Encryption Standard (AES) Algorithm

Advanced Encryption Standard (AES) also referred to as Rijndael, is a Symmetric Key block cipher algorithm. Advanced Encryption Standard (AES) came into existence to overcome the limitations of earlier famous and universally accepted Data Encryption Standard (DES). AES became the standard for the encryption and published by United States National Institute of Standards and Technology (NIST) in November 2001: FIPS PUB 197. AES existence was based on the competition carried out by NIST.

At the beginning and at the very end of AES a sub key is added, this process is known as "key whitening". First step of AES starts with key expansion, where cipher text is expanded to round keys. AES requires a different round key for each of its round according to key sizes. The next step is Add RoundKey, where XOR operation takes place between each byte and round key. Then executes the round according to the key sizes.in AES all rounds are identical except for the last round as shown in figure 2.

Each round consists of 4 layers:

1. Byte Substitution (ByteSub)
2. Shift Rows
3. Mix Columns (MixCol)
4. Key Addition

Last round of AES do not contain the Mix Column layer

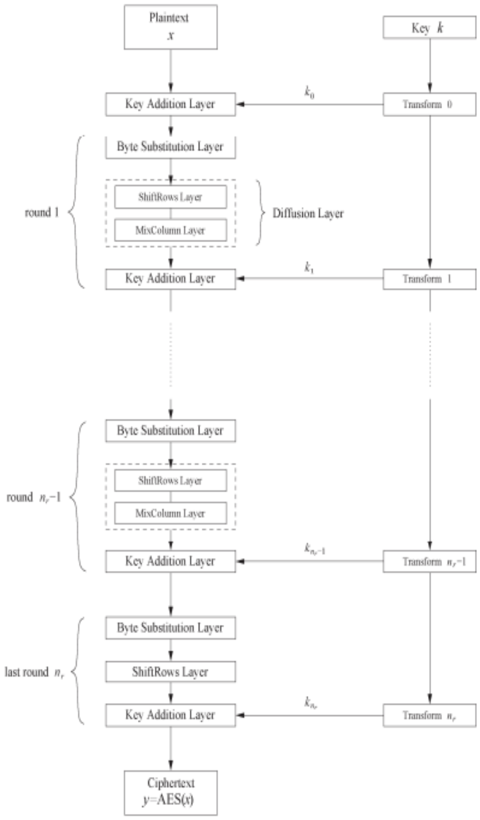

Figure 2 Steps for encryption in AES

5. RESULTS AND DISCUSSION

This section of the paper discusses the overall performance and the result of the proposed scheme after implementation on the cloud environment. The entire implementation of the work proposed was done in JAVA language with eclipse as an Integrated Development Environment (IDE) and is based on the socket programming in java. We have created the client and server part which communicate with each other with encrypted messages. The socket programming in java helps to create private cloud within same network, where the files of the user have been saved. The MySQL database is installed on the server side to validate and register the user details. At the time of login it checks the validation of the user in the database.

Since in the proposed scheme, there is new approach of authentication from both sides which makes the security much better as compared to other approach with little compromise with time as shown in figure 3. In the implementation of the scheme we used the Advanced Encryption Standard with random key for different files which will be known to user only and hence makes it difficult problem to break or find keys to decrypt stored files by the user. So this scheme will makes it more difficult to decrypt the files from attacker.

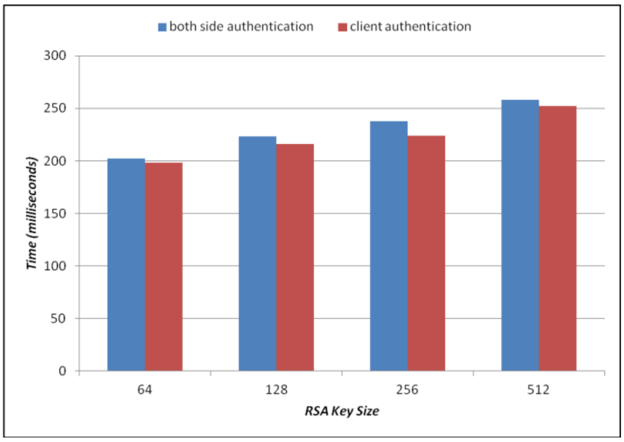

Figure 3 Time taken for bi-directional authentication

5. CONCLUSION AND FUTURE WORK

Cloud Computing is a well-known technology to provide services over the internet. Cloud act as Data Centre. A customer utilizes clouds resources and services and is charged accordingly. Security is the most important concern in cloud computing. There are various security issues of cloud computing which are related to trust, data confidentiality, authentication, access control etc. The impact of data security and the extent of loss that is suffered due to unauthorized access to cloud data motivates to take the problem as a challenge and come up with feasible solutions that can protect the data from theft, mishandling. Various authentication techniques are available in cloud computing but some are efficient in terms of time and some are attack resistant. In this paper we proposed a security technique for cloud computing environment that provides Bidirectional Authentication between clients and server. In the proposed technique, we used the Hybrid Encryption Algorithm involving RSA and AES with chaotic theory.

6. REFERENCES

[1] Prajapati, A., Rathod, A.: Enhancing Security in cloud computing using Bi-Directional DNA Encryption Algorithm. Springer(2015)

[2] Mahajan P., & Sachdeva A.: A Study of Encryption Algorithms AES, DES and RSA for Security. Volume 13, Issue 15, Version 1.0, GJCST(2013)

[3] Kumar S., R., G., Kannan, K. R.: Data Integrity and Security in Cloud Environment Using AES Algorithm. IJARCSSE(2013)

[4] Kaur, A., Raj, G.: Secure Broker Cloud Computing Paradigm Using AES and Selective AES Algorithm. Volume 3, Issue 3, IJARCSSE (March-2013)

[5] Pradhan, C., Bisoi, A.K.: Chaotic Variations of AES Algorithm. In: International Journal of Chaos, Control, Modelling and Simulation (IJCCMS) Vol.2, No.2, (June 2013)

[6] Chen, D., Zhao, H.**:** Data Security and Privacy Protection Issues in Cloud Computing. In: International Conference on Computer Science and Electronics Engineering (2012)

[7] Somani, U., Lakhani, K., Mundra, M.: Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing. In: 1st International Conference on Parallel, Distributed and Grid Computing (2011)

[8] Zhang, S., Zhang, S., Chen, X., Huo, X.: Cloud Computing Research and Development Trend. In: Second International Conference on Future Networks, IEEE (2010)

[9] Jensen, M., Schwenk, J., Gruschka, N., Iacono, L.L.: On Technical Security Issues in Cloud Computing. IEEE International Conference on Cloud Computing (2009)

[10] Mukhopadhyay, D., Sonawane, G., Gupta, P. G., Bhavsar, S., Mittal, V.: Enhanced Security for Cloud Storage using File Encryption

[11] Cao, Ning, et al. "Privacy-preserving multi-keyword ranked search over encrypted cloud data." *Parallel and Distributed Systems, IEEE Transactions on*25.1 (2014): 222-233.