Secure File Storage in Cloud using Transparent Cryptography Algorithm

Preethi V, Sudharsan K, Ajay Baskar KH, Sushil Ram T

Abstract – Cloud Computing is nowadays a growing market these days. The most common usage of cloud computing is backup, in which large amount of data is stored. There is a increased use of cloud computing in various organisations such as IT industries. When the user requests the data, it can be reclaimed from the cloud. For the security of data in cloud various techniques such as cryptography and stenography is used. For high level security to data in cloud computing a single algorithm won't be effective. A new security algorithm is proposed in this paper using Transparent key cryptography algorithm and stenography. The challenging issue in cloud computing is to provide security to the data stored in the cloud. The most popular Transparent key system is Data Encryption Standard (DES), Advanced Encryption Standard (AES), RSA and blowfish algorithms are used to provide security to the data .The cloud computing benefits in a way that accessing of data through internet with low cost. The multi threading technique is used to encrypt each and every part of the data using different type of algorithm.

Keywords –
Cloud Service Provider (CSP), Cloud Server (CS), Encryption/Decryption Procedure.

I. INTRODUCTION

The translation of original data into an non-readable form by protecting it from un authorised usage is called as cryptography. Keys are used to translate data into an unreadable form. So only the authorised user can access the data from cloud server. The cryptography algorithms are divided into two types. They are Transparent key algorithm and public key algorithm. Advanced Encryption Standard (AES), Data Encryption Algorithm (DES), blowfish, two fish, triple DES are some of the Transparent key cryptography algorithms. The delay in encoding and decoding of data is less in these algorithms and the security is low. The examples of public key cryptography algorithms are RSA and ECC. In these algorithms the security is very high in encryption and decryption but the delay is more.

The secret data is hidden by the Stenography into an envelope. Only the authorised user knows about the existence of the data. This text stenography technique is used to provide high level security to the data. Minimum space is enough for the text stenography when compared to that of the image stenography. The text encryption and decryption is done by the Data Encryption Standard (DES).

The image stenography uses three bit LSB procedure. This system is requested by author R.T.Patil. The secret data is hidden into the cover image using the LSB stenography procedure.The implementation of high throughput architrechture for cryptography algorithm is proposed by author Klauss Haffman. Advanced Encryption Standard (AES) is one of the Transparent cryptography algorithm. Three keys are supported by it.

In which ten rounds is required for 128 bit key, twelve rounds is required for 192 bit key and fourteen rounds is required for 256 bit key. The encryption and decryption time is reduced in improved AES algorithm. It provides better performance in terms of delay for the modified AES algorithm.

II. EXISTING SYSTEM

When the customer stores the data in cloud service provider there is an increase threat to the stored data. The existing system produce large squared errors. Four type of threat model comes to our consideration. The first one is the availability of data is affected when the server of cloud service provider is crashed. The second threat is data integrity in which the cloud service customer cannot completely rely on the cloud service provider. There are also many number of threats for the leakage of the data which includes hacking of cloud service provider or comprises of the cloud user accounts which concludes the third type of threat model. It is common that everyone doubts the third party, this problem is even bigger when it comes to business data and sensitive military data which could be hacked by other parties. The cloud is a multi-user environment in which also the resources are shared which doubts the security of the data stored. The existing system need some time for the encryption and the decryption process when compared to hybrid algorithm. Thus the effectiveness of the existing system algorithm is diminished.

III. PROPOSED SYSTEM

As shown in the figure the proposed system need at least some time for the file to encode. Because combination of several transparent key cryptography algorithm is used in the proposed system. AES requires less time for the file to encode when compared to that of the blowfish. It requires 12% to 15% time of encoding when compared to that of the blowfish in the proposed system. But blowfish need less

Revised Manuscript Received on April 25, 2019.

Ms.Preethi V,Assistant Professor (O.G), Department of Computer Science and Engineering, Ramapuram Campus, SRM Institute of Science and Technology (formerly known as SRM University) Chennai India

Sudharsan K,(Student), Department of Computer Science and Engineering, Ramapuram Campus, SRM Institute of Science and Technology (formerly known as SRM University) Chennai India

Ajay Baskar KH,(,(Student), Department of Computer Science and Engineering, Ramapuram Campus, SRM Institute of Science and Technology (formerly known as SRM University) Chennai India

Sushil Ram T (Student), Department of Computer Science and Engineering, Ramapuram Campus, SRM Institute of Science and Technology (formerly known as SRM University) Chennai India

time for the text file to decode when compared to that of the AES algorithm. The decryption need more time when compared to that of encryption in blowfish algorithm.

IV. SYSTEM ARCHITECTURE

The Architectural design of hybrid cryptography algorithm consists of the cloud user and cloud owner. First the cloud owner enters the data into the cloud server. Then the data uploaded in the cloud server is divided into eight parts. Each file is encrypted using different algorithm using the multi-threading technique. Cloud server stores the encoded file. Keys used for encryption purpose are stored into cover image. Multiple people are accessible to cloud computing where more than a single user is able to use file in the cloud server. The cloud user request for the file. On the request of the user also receives the cover image using e-mail in which the secret information is hidden. In this way the encryption process is done. The reverse process is used to decode.

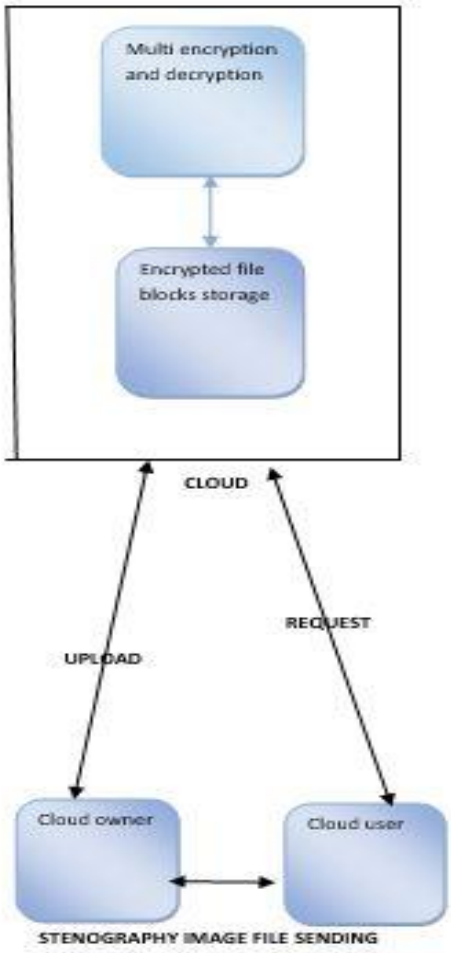

Fig 1. System architecture

V. FRAMEWORK

a) TRANSPARENT KEY CRYPTOGRAPHY

Encryption is used to convert the data into code word using algorithms. After encryption the code word will be converted again as a meaningful data, if anyone wants to access the data they should decrypt the data.

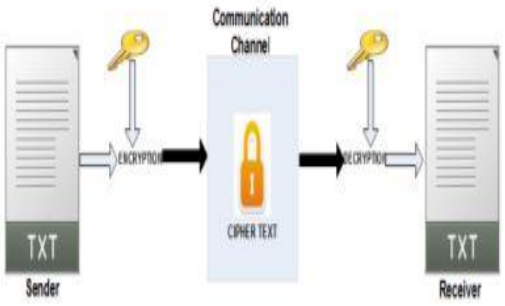

FIG .2 WORKING OF ENCRYPTION AND DECRYPTION

Suppose the data is stolen or coincidently shared with anonymous users still it is protected because it is unreadable. The meaning of transparent will differ from user to user. The encryption is managed by transparent encryption and the access is given to encryption keys where the overall process is made translucent to the user.

Transparent key cryptography encryption method takes place when both the sender and receiver share the same key. This was the only known method in encryption until June 1976. Transparent key code words are constructed as either block code or stream code. A block code encodes the input into block of plaintext as opposed to individual characters, stream code than uses the input. The deployment is simple scalable and fast with agents installed at operating system are device layer.

VI. EXPERIMENTAL RESULT ANALYSIS

Transparent key algorithm is the study of letters or groups of letters containing cod words. It will partially reveal the code word. Privacy plays a major role in transparent key algorithm so both the parties share the same key of encryption and decryption at the same time. No third parties are allowed to access the keys, if not the safety is lost. Evidently transparent key algorithm is not consuming much more computing power.

VII. CONCLUSION

Cloud storage problems are solved using transparent key algorithm technique. Data security for the cloud is done by using AES, DES, blowfish and RSA algorithm key information security is achieved using LSB algorithm and multithreading technique will be used for low delay parameter. We used encryption time and key generation time to evaluate the cryptographic schemes. These performance shows that the schemes are inexpensive when compared to other schemes. In future we plan to elaborate more schemes and extend our performance analysis results.

REFERENCES .

1. V.S. Mahalle , A. K. Shahade, “Enh.ancing the Data Security in Cloud by Implementing .Hybrid (Rsa & Aes) Encryption Algorithm”, IEEE , INP.AC,pp 146-149,Oct .2014..
2. Abu Marjan, Palash Uddin, “Developing Efficient Solution to Information Hiding through text steganography along with cryptography”,IEEE, IFOST,pages 14-17, October 2014.
3. P. S. Bhendwade and R. T. Patil, “Steganographic Secure Data Communication”,IEEE, International Conference on Communication and Signal Processing, pages 953-956,April 2014.

4. S. Hesham and Klaus Hofmann , "High Throughput
5. Architecture for the Advanced Encryption Standard
6. Algorithm" IEEE,International Symposium on Design and Diagnostics of Electronic Circuits & Systems, pages167- 170,April 2014.
7. M. Nagle, D. Nilesh, "The New Cryptography Algorithm with High Throughput",IEEE, ICCCI ,pages 1000000000000000000-5,January 2014.
8. ZhouYingbing, LI Yongzhen, "The Design and Implementation of a Transparent Encryption Algorithm Based on DES", IEEE,ICSESS,pages 517-520,June 2014.
9. N. Sharma ,A.Hasan, "A New Method Towards Encryption Schemes (Name-Based-Encryption Algorithm)",IEEE, International Conference on Reliability, Optimization and Information Technology,pages 310-313,Feb 2014.
10. Inder Singh, M. Prateek," "Data Encryption and Decryption Algorithms using Key Rotations N. Sharma,A.Hasan, "A New Method Towards Encryption Schemes (Name-Based-Encryption Algorithm)",*IEEE, International Conference on Reliability, Optimization and Information Technology*,pages 310-313,Feb 2014.
11. Jasleen K., S.Garg[,"Security in Cloud Computing using Hybrid of Algorithms",*IJERJS*, Volume 3, Issue 5, ISSN 2091-2730,pages 300-305, September-October, 2015.

AUTHORS PROFILE

Ms.Preethi V,Assistant Professor (O.G), Department of Computer Science and Engineering, Ramapuram Campus, SRM Institute of Science and Technology (formerly known as SRM University)

Sudharsan K,(Student), Department of Computer Science and Engineering, Ramapuram Campus, SRM Institute of Science and Technology (formerly known as SRM University)

Ajay Baskar KH,(,(Student), Department of Computer Science and Engineering, Ramapuram Campus, SRM Institute of Science and Technology (formerly known as SRM University)

Sushil Ram T (Student), Department of Computer Science and Engineering, Ramapuram Campus, SRM Institute of Science and Technology (formerly known as SRM University)