Cloud based Secure Storage of Files using Hybrid Cryptography and Image Steganography

Vinay Poduval, Ashish Koul, Daniel Rebello, Karunesh Bhat, Revati M. Wahul

Abstract: ***Cloud Computing has made it possible to provide individuals as well as organizations with a utility that is cost-effective. It empowers businesses by delivering these services using the internet. Files can be shared through the cloud. These files may contain sensitive information that needs to be kept hidden from anonymous users. This is done using cryptographic algorithms. High level of security can be provided using hybrid cryptography to encrypt the data. Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) are the symmetric key encryption algorithms used to secure. An asymmetric key encryption algorithm, Rivest-Shamir-Adleman (RSA) helps in providing a hybrid cryptography model. The security of the key generated can be further enhanced using image steganography method Least Significant Bit (LSB). These issues regarding the security and its challenges will be addressed in this paper and also analyse the measures to handle it.***

Keywords: Cloud Security, Cryptography, Encryption, Steganography.

I. INTRODUCTION

Cloud computing brings an innovative option to manage the data resources. Within this computing environments, the cloud servers can offer various data services, such as remote data storage and outsourced delegation computation etc. Since the cloud server may not be reliable, the file cryptographic storage is an effective method to stop private data from being stolen or altered. In the meantime, they may need to share data with the person who satisfies some requirements. To make such data sharing be possible, hybrid encryption is applicable.

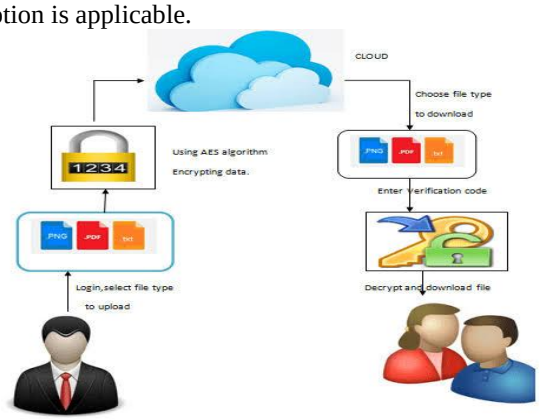

Fig.1 Encryption/decryption process of data sources

Revised Manuscript Received on March 15, 2020.

Vinay Poduval, Pursuing Bachelor's Degree, Computer Science, MES College of Engineering, Pune University.

Ashish Koul, Pursuing Bachelor's Degree in Computer Science, MES College of Engineering, Pune University.

Daniel Rebello, Pursuing Bachelor of Engineering (BE) degree, Computer, Modern Education Society's College of Engineering.

Karunesh Bhat, Pursuing, Bachelor of Engineering (BE) degree, Computer, Modern Education Society's College of Engineering.

Miss Revati M Wahul, Faculty, Computer Engineering, M. E. Society's College of Engineering, Pune.

At the Data owner side the data to be sent to the user/client is encrypted using various encryption techniques, but instead of using a single encryption technique we can use different encryption techniques by dividing the data into different parts. Then these encrypted files are used for the generation of secure key which further can be hided using robust image steganography and then sent to the user where the decryption is further done.

II. LITERATURE SURVEY

In paper author proposes a model using data hashed message authentication codes (HMAC) and index building for determining the errors and raises the efficiency. Performance of Encryption algorithms based on confidentiality, integrity and availability are also assessed. Various algorithms are discussed in this paper along with their and disadvantages. Author also discusses a technique by the use of Rivest Shamir Adleman (RSA) algorithm and MD5 to construct a protected atmosphere for cloud computing. Authors provide more trustworthy, precious and harmless atmosphere for cloud computing with use of combination of blowfish symmetric and RSA algorithm. The usage of above mentioned technique was able to reduce or overcome the issues of data security and primary issues in cloud. [1]

Author proposed the notion of attribute-based encryption (ABE). In subsequent works, they focused on policies across multiple authorities and the issue of what expressions they could achieve. Author also proposed the generic KEM/DEM construction for hybrid encryption which can encrypt messages of arbitrary length. Based on their ingenious work, a one-time MAC were combined with symmetric encryption to develop the KEM/DEM model for hybrid encryption. [2]

The proposed framework given an original image and the secret data to be hidden, our purpose is to generate an intermediate image whose channel compressed version is exactly the same as the stego-image. To this end, we first obtain the stego-image by data embedding on the channel compressed original image using any of the existing JPEG steganographic schemes. Then, we propose a coefficient adjustment scheme to produce the intermediate image based on the stego-image and the original image. This scheme ensures that the channel compressed version of the intermediate image is exactly the same as the stego-image. [3]

III. PROPOSED METHODOLOGY

In the proposed model Hybrid Cryptography along with Image Steganography is used. AES, DES, 3DES, BRA are some of the symmetric key cryptography algorithms.

A symmetric key algorithm requires only a private key to encrypt and decrypt the data and no public keys are required. Hence it is less secured as during the transmission of the key there is a possibility of the communication channel to be tapped. Along with this, several public key encryption algorithms such as RSA, ECC also exist.
The main disadvantage of public key cryptography is that it increases delay to encode and decode data. Although it makes use of both public and private key, it is more secure than the symmetric algorithms. The figure 2 illustrates the hybrid cryptography mechanism.

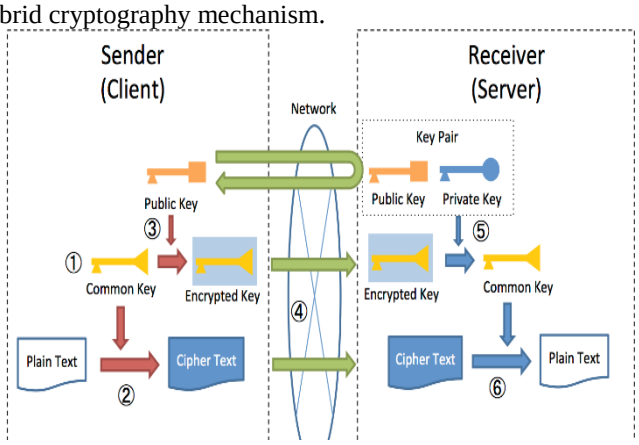

Fig.2 Hybrid Cryptography Model

To remove the drawbacks of the symmetric and public key algorithms a hybrid cryptography model can be used. This model would make use of the symmetric as well as public cryptography techniques in order to provide a highly secure model. Two symmetric algorithms, AES and 3DES; and RSA, a public key algorithm are used for this purpose.

Step 1. First, the data is secured using the symmetric algorithms AES and 3DES. A secret key is generated due to this.
Step 2. The key obtained from step 1 is further secured and encrypted using RSA which is a public key encryption technique.

Step 3. The public key thus obtained after step 2 is embedded into an image using the image steganography technique – LSB. Figure 2 illustrates image steganography technique.

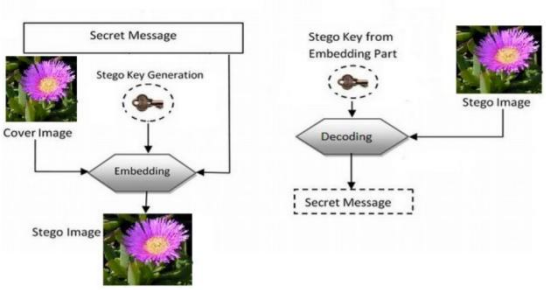

Fig.3 Image steganography technique

When a user requests for a file, the administrator provides the user with the stego image consisting of key information. User then decrypts the stego image to receive the information stored in the image, i.e. the public key information. User then decrypts that to obtain the symmetric key. This key is decrypted finally to obtain the original data. The decryption process is the exact reverse process of encryption.

IV. RESULTS AND DISCUSSIONS

Using the technique of encryption and decryption algorithms for the storage of the files, the efficiency of the algorithms will be checked, more secure storage of the files will be made possible and which algorithm performs a better encryption/decryption of the message is checked. Instead of using a single algorithm for the storage, the use of multiple algorithms are implemented for the file (AES, RSA & 3-DES) due to which there is an increase in the security of the file. The efficiency of the algorithms can be determined based on the methodology used to protect the file. The use of 3-DES algorithm has been done in this paper; it is more preferred as it provides higher levels of security as compared to the DES algorithm. 3-DES uses three keys for the encryption process which shows additional rounds as compared to a single key which is used for DES.

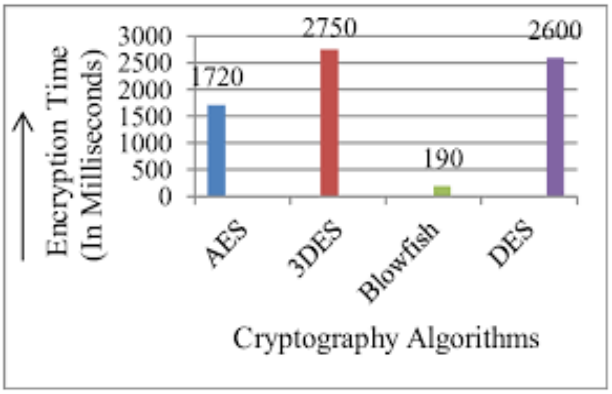

Fig.4 Comparison of various Cryptography Algorithms[1]

For the image steganography algorithm, the encrypted text of the file will be sent to the user's email account with the respective image. Whenever he/she requires to access the contents of the file then the stego-image will be used to start the decryption process in which the hidden text will be decrypted. There will be different ways in which the decryption of the text will take place based on the image provided along with it. In case of greyscale images, the algorithm offers a large payload capacity and can provide high levels of security and even higher invisibility levels. For the colour images, it achieves the same levels of security and invisibility of the hidden text. Furthermore, the technique used here is more efficient and gives better results in comparison to the proposed technique used in the previous algorithm.

V. CONCLUSION

This paper proposes the working of the hybrid cryptography and image steganography algorithms for the secure storage of files on the cloud. This technique helps in achieving higher efficiency and better security due to the use of multiple algorithms for the encryption/decryption process. Added work on this paper, the use of 3-DES algorithm has been done for the encryption purpose for getting suitable results and achieving higher security for the transmitted data. High level security of data is required in banking and private sectors where the proposed system can be used.

Furthermore, work can be done in order to improve the time taken to secure the files using the encryption techniques used whilst providing the same level of security.

REFERENCES

1. Jie Xu, Qiaoyan Wen, Wenmin Li and Zhengping Jin; "Attribute-based
2. Hybrid Encryption in Cloud Computing"; IEEE Transactions on Parallel and Distributed Systems; 2016
3. Jinyuan Tao, Sheng Li, Xinpeng Zhang and Zichi Wang; "Towards Robust Image Steganography"; IEEE Transactions on Circuits and Systems; 2018
4. Surabhi Singla and Anju Bala; "Cryptography and Steganography Algorithms for Cloud Computing"; ICICCT 2018
5. J. Li, X. Huang, J. Li, X. Chen and Y. Xiang; "Securely Outsourcing Attribute-based Encryption with Checkability"; in Proc. IEEE Transactions on Parallel and Distributed Systems,
6. 2013.
7. V.S. Mahalle, A. K. Shahade; "Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm"; IEEE INPAC 2014
8. Jasleen K, S.Garg; "Security in Cloud Computing using Hybrid of Algorithms"; IJERJS, ISSN, 2015.
9. S. Li and X. Zhang; "Towards construction based data hiding: From secrets to fingerprint images"; IEEE Transactions on Image Processing; 2018
10. Cao, N., Cong Wang, Ming Li, Kui Ren and Wenjing Lou; "Enhanced Privacy-Preserving Multi Keyword Ranked Search over Encrypted Cloud Data"; IEEE Transactions on Parallel and Distributed Systems; 2015

AUTHORS PROFILE

Vinay Poduval is a student from MES College of Engineering, Pune University and is pursuing his Bachelor's degree in Computer Science. He will graduate with a BE degree in May-2020. His interests include web development, networking and security. He is a certified full-stack web developer and is eager to learn new technologies.

Ashish Koul is a student from MES College of Engineering, Pune University and is pursuing his Bachelor's degree in Computer Science. He will graduate with a BE degree in May-2020. His interests are Security algorithms and cloud computing. He gave a seminar on the topic of multi-tenancy in cloud computing.

Daniel Rebello is pursuing his Bachelor of Engineering (BE) degree in Computer from Modern Education Society's College of Engineering. His research interests are Cloud Computing, Data Science and cryptography. The technical coding languages known to him are C, C++ and Python.

Karunesh Bhat is pursuing his Bachelor of Engineering (BE) degree in Computer from Modern Education Society's College of Engineering. His research interests are Cryptography and Cloud Computing. The technical coding languages known to him are C, C++ and PHP.

Miss Revati M Wahul is from Aurangabad in Maharashtra state of India. She completed Bachelor's degree in Computer Science & engineering from Dr. BAMU University, Aurangabad in 2002 & Master's degree in Computer Engineering in 2010 from Dr. BATU University, Lonere. She is pursuing her PhD in Computer Science & Engineering from Dr. BAMU University, Aurangabad. She is working as faculty in Computer Engineering at M. E. Society's College of Engineering, Pune since 2005. She has published number of research papers in international / national conferences and journals. Her area of interest include Cloud Computing, Microprocessors, Project Management, Big data, IoT.