INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 05 ISSUE: 06 | JUNE - 2021 ISSN: 2582-3930

Secure File sharing using Hybrid Cryptography and Image steganography

Paras Kamble, Ganesh Patil, Snehal Maliya, Aniket Nimbalkar
Computer Department of Engineering,
JSPM BSIOTR, WAGHOLI,
PUNE, INDIA.

Abstract— In this paper we have discussed about the proposed system which uses hybrid algorithm which we can use to securely share the data on the internet. Due to the huge amount of data on the internet, the need for security has been increased in the current era. The moment we share our information by any means of communication such as internet, telephone, postcard it's the responsibility of that service provider to share it securely with the receiver. But once it's leaked worldwide, we can't do anything about it. So, we can imagine how Security can be considered as the superior priority for sharing sensitive files of any organization, government-related intel, database of a bank server. These databases require a higher security concern while sharing the data. Therefore, to overcome this issue we have made our Proposed system. In our system, we share the data by encrypting it using Hybrid cryptography as a key factor of our system and then sharing our secret data using image steganography which works as a cherry on top. So even if the hacker is trying to steal our data, he/she won't be able to know what we are trying to share because of the use of Hybrid cryptography. We have used 3 algorithms which are AES, 3DES, Blowfish in our proposed system to encrypt the data into a compressed file and that file is kept hidden in our image using image steganography.

Index Terms— Security, Hybrid cryptography, AES, 3DES, Blowfish, Image steganography.

1 INTRODUCTION

The more the amount of data the more is the risk of getting hacked. Because of the information and technology, the size of data is increasing on the internet day by day so the need for security has also been increased. So, we can imagine how the data needs to be secured when we are sharing any sensitive data of any bank server, or any military-related documents. To share the data from sender to receiver we have been using a concept called cryptography from 400 BC with the help of a scytale. This concept was used by Spartans at that time to share military-related information. Since then, we are using cryptography for sharing and receiving data by using different algorithms, as this technology is known to us for such a long period of time it also has certain drawbacks that such as we know how the algorithms how to crack them but this kind of things happens with every other technology in the market because everything has an answer, we just have to search harder. So, to overcome the problem of data getting cracked and then leaked by hackers we have used Hybrid cryptography to encrypt the data in our proposed system and have store it using image steganography in an image so that we won't get stuck in any kind of suspicion by the hacker who is trying to steal it.

Cryptography is a concept used for encryption and decryption of the data for sharing, storing, and receiving it. We are familiar with the technology named Cryptocurrency this technology also uses cryptography along with Block-chaining to transfer and receive money. In our system, we have used Hybrid cryptography so that even if our data is stolen the person won't be able to detect which algorithm we have used in our system for encryption as we have used 3 algorithms to encrypt a single message. We have used AES, 3DES, Blowfish algorithms in a parallel manner to convert our message into ciphertext, and then we have used image steganography to hide our encrypted data in a zip file inside an image.

Image steganography is a concept that is used to share any information which we don't want to reveal to anyone. As the name itself has steganography in it, it's used to share data inside another data. This concept is also an old-age technology which has developed by ancient Greeks. Therefore, we have combined those technologies (cryptography & steganography) and have used them in our proposed system to create something new by modifying the old.

2 LITERATURE SURVEY

1. SECURE FILE STORAGE ON CLOUD USING CRYPTOGRAPHY

Authors: Joseph Selvanayagam, Akash Singh, Joans Michael, Jaya Jeswani.

Description: In this paper we aim to securely store information into the cloud, by splitting data into several chunks and storing parts of it on cloud in a manner that preserves data confidentiality, integrity and ensures

availability.

2. Secure File Storage on Cloud using Cryptography

Authors: Paras Kamble, Ganesh Patil, Snehal Maliya, Aniket Nimbalkar.

Description: In this paper, we have reviewed a system that has a hybrid algorithm mechanism to store and secure the data in the cloud and transfer it, so even if there's any security breach the hacker won't be able to find out which algorithm was used to encrypt the data.

3. Secure File Storage on Cloud Using Hybrid Cryptography Algorithm

Authors: Uttam Kumar, Mr. Jay Prakash.

Description: Cloud is used in various fields like industry, military, college, etc. for various services and storage of huge amount of data. Data stored in this cloud can be accessed or retrieved on the users request without direct access to the server computer. But the major concern regarding storage of data online that is on the cloud is the Security.

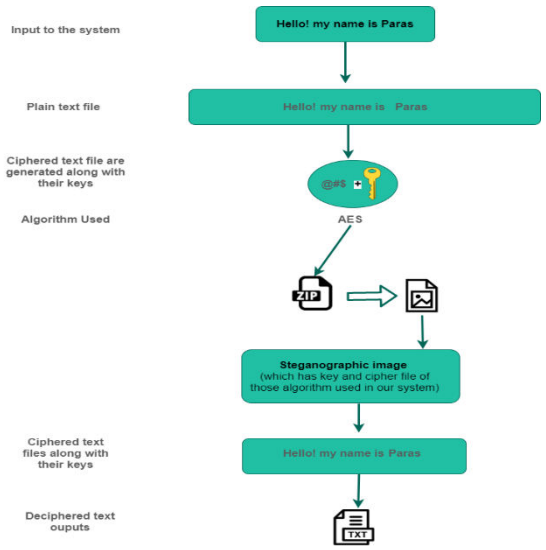
4. Secure File Storage on Cloud using Hybrid Cryptography

Authors: Aditya Poduval, Abhijeet Doke, Hitesh Nemade, Rohan Nikam.

Description: In this era cloud computing is used in various fields like industry, military, college, etc. for various services and storage of huge amount of data. Data stored in this cloud can be accessed or retrieved on the users request without direct access to the server computer.

3 EXISTING SYSTEM

The existing system had only one algorithm which was using a single key for encryption as well as decryption so if the key got leaked or let's say our encrypted message is cracked easily.



So as everyone knows the encryption format of a particular algorithm in cryptography one can easily crack the data by applying brute force attack on a higher performance hardware system to fetch our data. Peoples like crypto-analysts can easily get to know what kind of data we are sharing by just looking at our cipher text.

3.1 Disadvantages of the Existing system:

1- Only one algorithm was used to encrypt and decrypt the data which made it easy for the hacker to detect which algorithm is used for encryption.
2- Not efficient for higher security.
3- Higher chance of leaking of data if the hacker got to know which algorithm we have used in the system.

Fig: Existing system

4 PROPOSED SYSTEM & METHODOLOGY

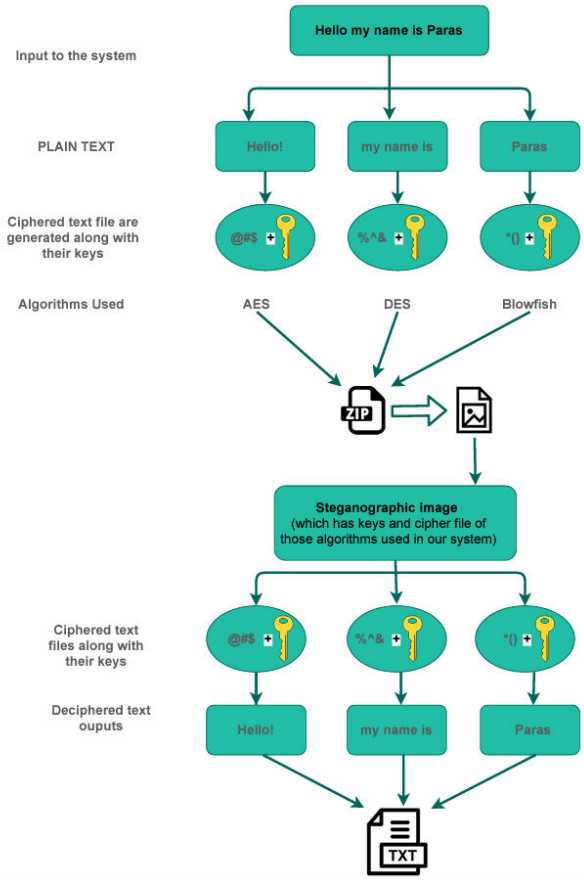


Fig: Proposed system

In our proposed system we have used hybrid cryptography which has 3 different algorithms i.e., AES, 3DES & Blowfish. These algorithms are applied for encryption to cipher a single message. Basically, what cipher means is to convert a plain text into some random gibberish symbolic text which doesn't relate to the given input. As we can see in the above diagram, we create these ciphertexts using 3 algorithms at a time. The ciphertext is not created unless and until we don't have a key for that encryption. This key is also shared with the receiver so even if the cipher file is leaked, we won't be able to decrypt our message without the key. These files having key file along with the cipher file is compressed in the zip file are stored in an image by hiding it into that image. At receivers' side these files are retrieved from the image shared and used for decryption of the message. This system was built to overcome the problem of data getting leaked even after encryption so that the hacker won't be able to get what kind of encryption algorithm is used to cipher the data. And to increase the security we have used image steganography to share the files required for decryption. And when the cipher file is decrypted, we are able to fetch the data in one single text format file as in was stored at the sender's side. This is the main purpose of our proposed system to share the files using these technologies.

METHODOLOGY

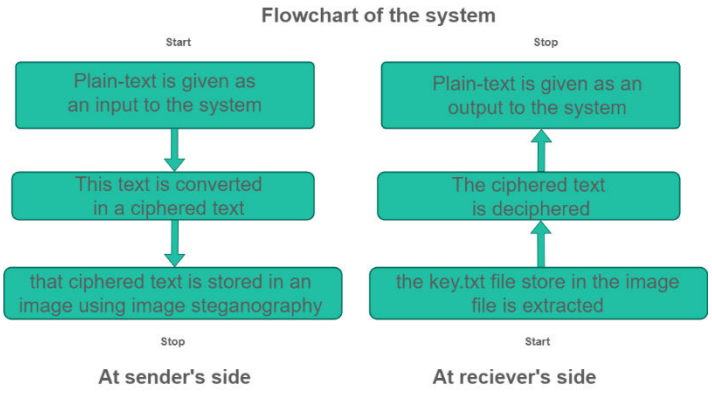


Fig: Flowchart of the system

This is the flowchart of our system where we can see how the system works in proper steps. At the sender's side plain text is converted into cipher text using algorithms with the permission of respected keys then these files (key files, ciphertext files) are stored into a zip file and that zip file is kept hidden and shared with the receiver using image steganography. At the receiver's side, that zip is extracted from the image along with its content and then it's further used for decryption to read the given message.

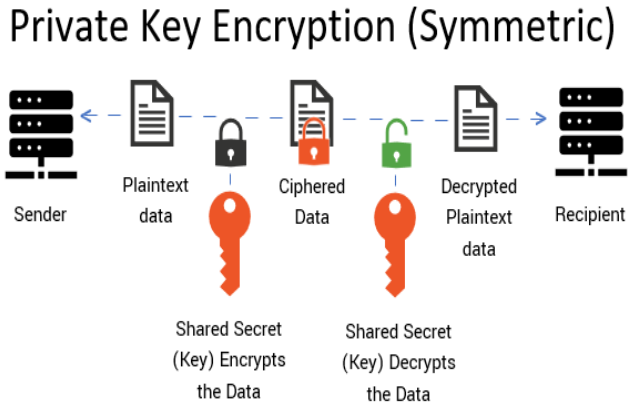
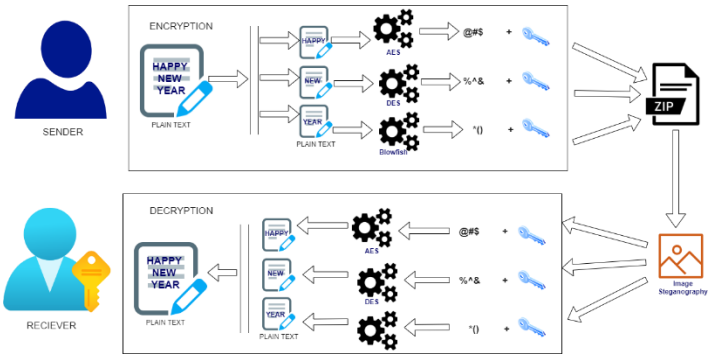


Fig: Symmetric key system

This is the representation how the algorithm works where at encryption it takes the input uses key encrypts it uses the key



again to decrypt it too and we get the message.

Fig: Architecture of the system

This is the architecture of the system which is explained in the above diagram

5 ALGORITHMS USED

AES (Advance Encryption Standard):

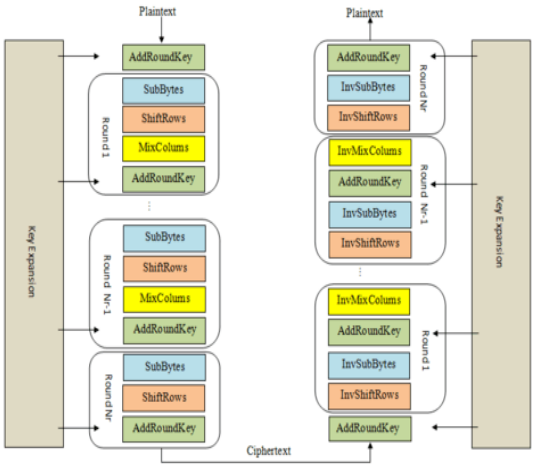


Fig: AES algorithm

AES algorithm is considered as one of the strongest algorithms to cipher the data where the key is used at the time of encryption as well as decryption. This algorithm was developed by Vincent Rijmen and Joan Daemen in October 2000 with the help of Rijndael block cipher in 1998. In this algorithm, 128 bits block size is ciphered by using a key whose sizes differ from 128 bits, 192 bits, or 256bits. Where depending on the key sizes the rounds of the process in the algorithm are repeated i.e., for 128 bits key 10 rounds, for 192 bits 12 rounds, and for 256bits 14 rounds. Each round has certain processing on the data as we can see in the above diagram First key is added in the block of 128-bit size then sub-bytes are added which is padding for adding certain bytes to make it more complex than rows and columns in which the block is stored is moved from its position
and then these rounds are repeated depending on the key size. The algorithm won't work if the padding provided is not correct at the sender and receiver side as well.

3DES (Triple Decryption Encryption Standard):

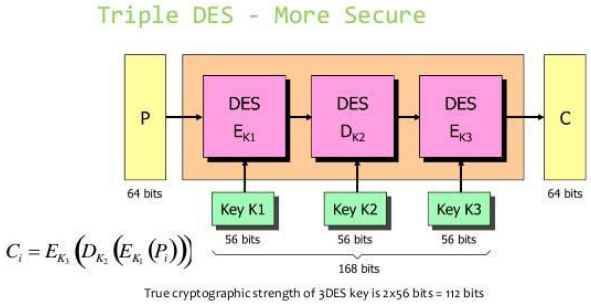


Fig: 3DES algorithm

As the name itself defines this algorithm just encrypt and decrypt the data given to it. It has a key of 64 bits but it only uses 56 bits of the key for ciphering the data. The implementation of this algorithm is easy to understand because it takes the input encrypt, decrypt and then encrypt it again and this step is repeated three times which is just basically DES but three times hence the name 3DES. It was made by using Lucifer cipher.

Blowfish algorithm:

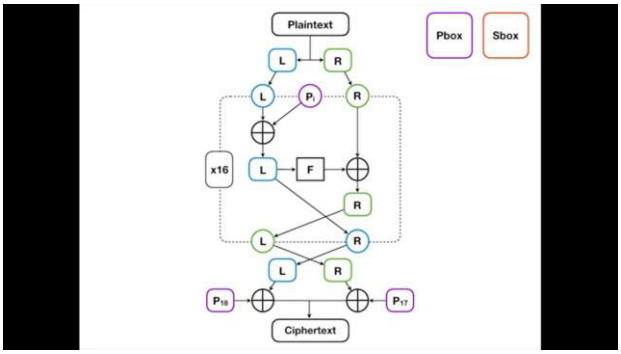


Fig: AES algorithm

It was developed by Bruce Schneier in 1983 which was a modification of DES where its key sizes differ from 32–448 bits and block size is of 64 bits. There is not a record of cracking it using brute force attack till now. It basically uses math magic where it XOR's the LHS and RHS of the plaintext and also uses on function while encrypting it by using XOR in that function too.

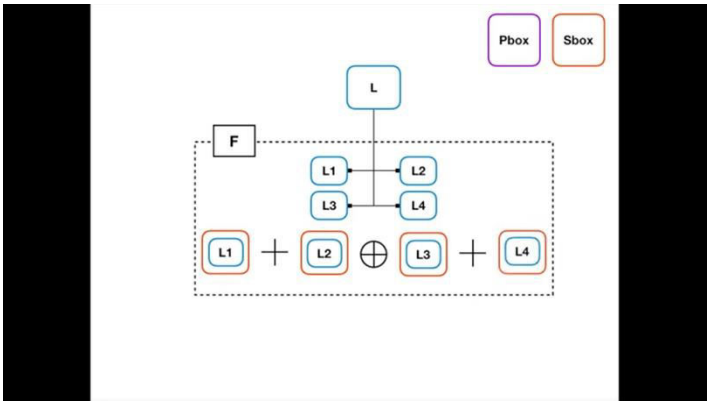


Fig: Blowfish algorithm

This diagram is the representation of the function used in Blowfish for increasing the complications and making the encryption as complex as possible.

6 RESULT & CONCLUSION

The aim of this proposed system is to securely store the data and share it by making it impenetrable even if the algorithms get cracked in the future by some advanced technology. AES, 3DES and Blowfish are the legendary algorithms which are used to encrypt the data and haven't been cracked till the present date but as every algorithm has some disadvantages which are not been discovered yet. Hence to overcome this issue we have used hybrid cryptography in our proposed system as well as image steganography to make it impossible to crack our data which we are sharing using our system.

7 REFERENCE

[1] Selvanayagam, J., Singh, A., Michael, J., & Jeswani, J. (2018). Secure file storage on cloud using cryptography. International Research Journal of Engineering and Technology, 5(2), 2044–2047.

[2] Poduval, A., & others (2019). Secure File Storage on Cloud using Hybrid Cryptography. International Journal of Computer Science and Engineering, 7.

[3] Kanatt, S., Jadhav, A., & Talwar, P. Review of Secure File Storage on Cloud using Hybrid Cryptography.

4] Mahalle, V. S., & Shahade, A. K. (2014, October). Enhancing the data security in cloud by implementing hybrid (RSA & AES) encryption algorithm. In 2014 International Conference on Power, Automation and Communication (INPAC) (pp. 146-149). IEEE.

5] Uddin, M. P., Saha, M., Ferdousi, S. J., Afjal, M. I., & Marjan, M. A. (2014, October). Developing an efficient solution to information hiding through text steganography along with cryptography. In 2014 9th International Forum on Strategic Technology (IFOST) (pp. 14-17). IEEE.

8 AUTHORS

First Author – Paras Sanjay Kamble, pursuing BE(Comp), JSPM BSIOTR (Wagholi) Pune,
Second Author – Snehal Maliya, pursuing BE(Comp), JSPM BSIOTR (Wagholi) Pune.
Third Author – Ganesh Kishore Patil, pursuing BE(Comp), JSPM BSIOTR (Wagholi) Pune.
Fourth Author – Aniket Nimbalkar, pursuing BE(Comp), JSPM BSIOTR (Wagholi) Pune.