ADVANCED DATA SECURITY IN CLOUD COMPUTING BY AES AND DES HYBIRD ALGORITHM

B.Balakumar, Assistant Professor,

Centre For Information Technology and Engineering,

Manonmaniam Sundarnar university,tirunelveli-627012 ,

Tamil nadu,India ,balakumarmsu@gmail.com.

G.Vinoth Ramkumar,*

Centre For Information Technology and Engineering,

Manonmaniam Sundarnar university,tirunelveli-627012,

Tamil nadu ,India , rram9695@gmail.com.

Abstract:

Information security is the most challenging issue in recent days. Cloud computing is used to implement security in many areas such as industries, institutions, military etc. Cloud computing providing resources to the areas over internet as per their requirements. Using a single algorithm is not suitable for high level security in cloud computing. Many systems consists of hybrid cryptography and steganography techniques. Both are the most popular now-a-days for high level data security. In this work, we propose a system with hybrid AES and DES algorithms to provide security to data. The hackers obtain stego text and they try to extract the original message. So we made this new algorithm using AES and DES make use of 128 bits key and increase in key length provides high security. Moreover, the data recipient can reconstruct the requested data from cloud computing server. We analyses and demonstrate the privacy protection of outsourced data is carried out on the repository of text files with variable size. This analysis shows that the proposed system a highly efficient for high data security in cloud systems.

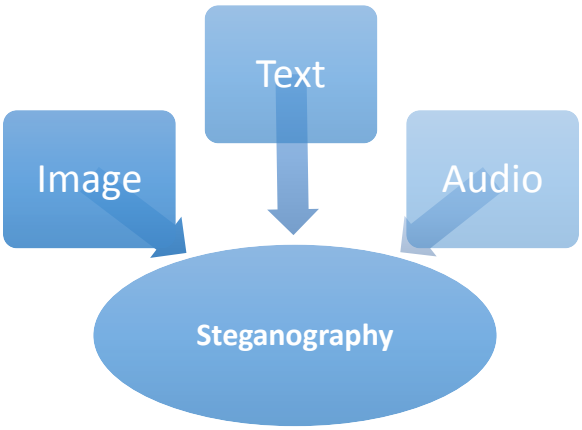
Keywords:

Security, Cloud computing, DES, AES, Steganography.

Introduction:

Security is one of the most difficult task to implement in cloud computing. The following paper first encrypts the plain text to cipher text using one of the existing algorithm available in the market. Once the Cipher Text is generated, the Cipher text with the cover text is used to create a stenographic text also known as stego-text. As the text message is encrypted using AES algorithm and embedded in a part of the image the text message is difficult to find. More over since the secret image is broken down into parts and then sent to the receiver. To encrypt the data various cryptographic algorithms such as DES. DES and AES can help to encrypt and decrypt the same process.

Steganography:



Text Steganogarphy:

It hides the text behind some other text file. It is a difficult form of steganography as the redundant amount of

text to hide the secret message is scarce in text files.

Image Steganography:

It is one of the most commonly used technique because of the limitation of the Humanvisual System(HVS). Human eye cannot detect the vast range of colors and an insignificant change in the quality of an image that results from steganography.

Audio Steganography:

It is also a difficult form of steganography as humans are able to detect a minute change in the quality of audio.

Image and audio captions (or annotations) may require a large amount of data. Annotations often travel separately from the host signal, thus requiring additional channels and storage.

Applications:

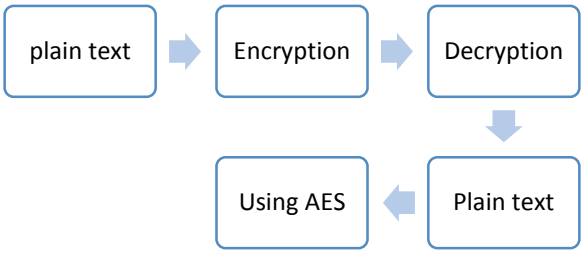
Image Steganography has many applications, especially in today's modern, hightech world. Privacy and anonymity is a concern for most people on the internet. Image Steganography allows for two parties to communicate secretly and covertly. It allows for some morally-conscious people to safely whistle blow on internal actions; it allows for copyright protection on digital files using the message as a digital watermark. One of the other main uses for Image Steganography is for the transportation of high-level or top-secret documents between international governments. While Image Steganography has many legitimate uses, it can also be quite nefarious. It can be used by hackers to send viruses and trojans to compromise machines, and also by terrorists and other organizations that rely on covert operations to communicate secretly and safely.

Algorithms:

Data Encryption can be performed by using two types of algorithms. One is symmetric key and other is asymmetric key algorithm. Symmetric key algorithms are widely used due to less complexity and faster processing as compared to asymmetric key algorithm.

Advanced Encryption Standard:

AES is a symmetric block cipher that can encrypt and decrypt information. The AES is capable of cryptographic keys of 128,192 or 256 bits. Other input, output, cipher key.



AES Process:

This algorithm may be used with the three different "flavors" may by referred to as "AES-128", "AES-192", and "AES-256". The input to each round consists of a block of message called the state and the round key . It has to be noted that the round key changes in every round. The state can be represented as a rectangular array of bytes. This array has four rows; the number of columns is denoted by Nb and is equal to the block length divided by 32. The same could be applied to the cipher key. The number of

columns of the cipher key is denoted by Nk and is equal to the key length divided by 32. The cipher consists of a number of rounds - that is denoted by Nr - which depends on both block and key lengths . Each round of AES encryption function consists mainly of four different transformations:

ByteSub Transformation:

The ByteSub transformation is a non-linear byte substitution, operating on each of the state bytes independently. The ByteSub transformation is done using a once-pre-calculated substitution table called S-box. That Sbox table contains 256 numbers (from 0 to 255) and their corresponding resulting values.

Shift Row Transformation:

In ShiftRow transformation, the rows of the state are cyclically left shifted over different offsets. Row 0 is not shifted; row 1 is shifted over one byte; row 2 is shifted over two bytes and row 3 is shifted over three bytes.

Mix-Column Transformation:

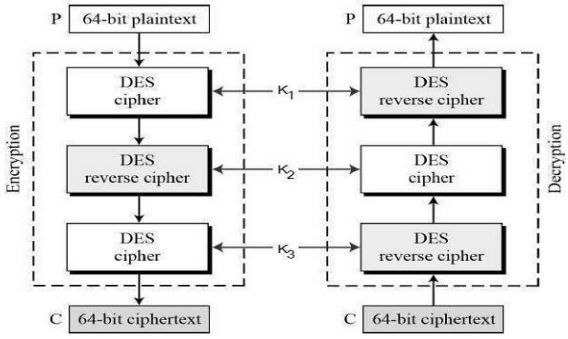
It operates on each column individually. It takes all the columns of the state and mixes their data to produce new column.

Add Key Transformation:

The round key is applied to the state - resulted from the operation of the Mix-Column transformation - by a simple bitwise X-OR. The round key length is equal to the block length. Each Round Key consists of Nb words from the key schedule. Those Nb words are each added into a column of the state. The output of the above transformations is called the 'state'. The state consists of the same byte length as each block of the message.

Data Encryption Standard:

Data Encryption Standard means to encrypt plaintext on the basis of standard that was developed. There is some critical data used for encryption and decryption know as a key. The algorithm used to encrypt data is a standard algorithm. Using standard algorithm data can encrypted and decrypted.



DES process:

This DES algorithm uses symmetric. block cipher for encrypting and decrypting data. Encryption converts data into gibberish language called cipher text. Decrypting the cipher text gives us back the original data that is plaintext. Converting the information from cipher to plain we use a standard form of algorithm called Symmetric algorithm.

DES takes an input of 64bits and the output is also of the same size. The process requires a second input, which is a secret key with length of 64bits. Block cipher algorithm is used where message is divided into blocks of bits. Block cipher is used for encryption and decryption. These blocks of bits are put through substitution, transposition, and other different mathematical functions.

Result Analysis:

Step1:

We have selected one image or audio file.

Step2:

And then in this step we can select the text document or we newly create the text documents is to be selected.

Step3:

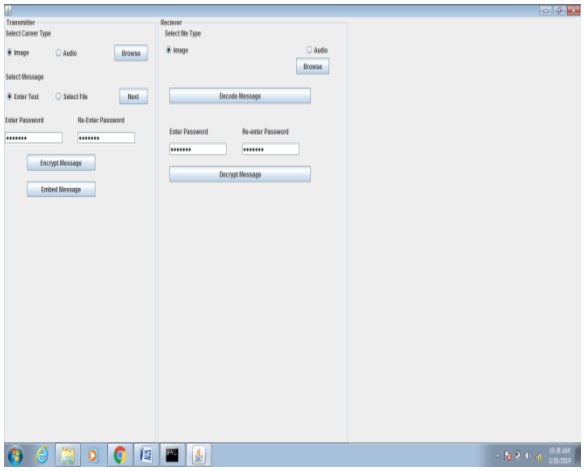
You create any password then re-enter password.

Step4:

We are applying two algorithm AES and DES. Finally hiding the text file into image or audio file .So this is called encryption.

Step5:

Already sent the image file received the receiver. Then moreover enter the password and decode message. In additional according to our methods was demonstrated. Then extract the text file is placed. Because each text file is placed at image file or audio file. This due to the decrypt message. The final output is



Conclusion:

The concept of cryptography long with encryption and decryption is explained. In this paper in embedding phase the encrypted message is embedded on to a part of the secret image or audio and the cipher text that is given as input in the text editor is actually hidden in the cipher and then in decrypted phase the encrypt image or audio is captured and then decrypt the image or audio and finally shows the output with decrypt messages.

References:

[1] This full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET 2016 conference." Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm".

[2] V.S. Mahalle , A. K. Shahade, "Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm", IEEE , INPAC,pp 146-149,Oct .2014

[3] Kiruthika.R,Jeena.R , " Enhancing Cloud Computing Security using AES Algorithm", IJARCSSE, Volume 5, Issue 3, ISSN 2277 128X,pp 630-635, March 2015.

[4] Inder Singh, M. Prateek," "Data Encryption and Decryption Algorithms using Key Rotations N. Sharma ,A.Hasan, "A New Method Towards Encryption Schemes (Name-BasedEncryption Algorithm)",IEEE, International Conference on Reliability, Optimization and Information Technology,pages 310-313,Feb 2014.

[5] "Secure Image Hiding Algorithm using Cryptography and Steganography" Ms. Hemlata Sharma,Ms. MithleshArya, Mr. Dinesh Goyal Department of Computer

Science and Engineering Suresh GyanViharUniversity, Jaipur Assistant Professor,Department of Computer Science &Engineering,Maharishi Arvind Institute ofEngineering&Technology.

[6] NOVEMBER 2015 " Trust Enhanced Cryptographic Role-Based Access Control for Secure Cloud Data Storage" Lan Zhou, Vijay Varadharajan, and Michael Hitchens

[7] 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.

[8] Abu Marjan, Palash Uddin, "Developing Efficient Solution to Information Hiding through text steganography along with cryptography",IEEE, IFOST,pages 14-17, October 2014.

[9] ZhouYingbing, LI Yongzhen, "The Design and Implementation of a Symmetric Encryption Algorithm Based on DES", IEEE,ICSESS,pages 517-520,June 2014.

[10] JAN-March 2018 " Developing an Efficient Solution to Information Hiding through Text Steganography Along with Cryptography" 1Venkata Bhanu Chowdary Allada, 2Mallikarjun Susarla 1,2Dept. of CSE, GITAM University, India.