HIGH LEVEL SECURITY IN CLOUD USING HYBRIDISATION OF PUBLIC KEY CRYPTOGRAPHY

[1]G.Umasowjanya, [2]G.Kumari

[1,2]Dept. of CSE, Pragati Engineering College,ADB Road, Surampalem, EG.dt, AP, India

ABSTRACT:

Data sharing has been tremendously increasing now a days and it's been very procedural structure to share data some of the important practices over a network might be risky. Cloud computing is the way to store, manage and process data in a convenient manner. For storing the data on a cloud is not much easy and have to face issues. To overcome, some techniques have to be implemented such strategies include cryptography and steganography. These techniques are secured and safer as well for sharing the data. Cryptography techniques translate the data into code text while steganography hide the data existence into envelope. Decryption and encryption have been done using AES, blowfish etc., algorithms for better results within the time and secured way as well.

KEYWORDS: Cryptography, steganography, encryption

1] INTRODUCTION:

Cryptography strategy makes an translates of unique data into ambiguous structure. Cryptography procedure is isolated into symmetric key cryptography and public key cryptography. This strategy utilizes keys for make an interpretation of data into unreadable form. So just approved individual can get to data from cloud server. Cipher text data is noticeable for all people.

Steganography hide the secret data presence into envelope. In this procedure presence of data isn't obvious to all individuals. Just legitimate recipient thinks about the data existence. Three bit LSB methods utilized for image steganography. This framework is recommended by creator R.T.Patil. Sensitive data of user stow away into cover image. We can hide huge amount of data into picture using LSB steganography strategy. The author Klaus Hafmann has actualized high throughput design for cryptography algorithm. AES is symmetric key cryptography algorithm. It underpins three sorts of keys. For 128 bit key require 10 rounds,192 bit key require 12 rounds and 256 piece key require 14 rounds. In improved AES algorithm encryption and decoding time is reduced. Advantage of changed AES algorithm is gives better execution as far as delay.

2] LITERATURE SURVEY:

2.1] R. Wu, G.-J *et al*

We have proposed an format-based pure text steganography algorithm including a private key cryptography giving a more elevated level of security. The cover text has been made as conventional as could be expected under the circumstances. After successful embedding of the secret message into the cover text, the stego-text likewise resembles a ordinary text on the grounds that lone an alphanumeric puzzle is included toward the end of the cover text content to make up the stego-text. This last stego-text is sent to the receiver through the unsecured correspondence channel. Rather than right recipient, if any outsider or wafer or programmer gets the stego-text, they may imagine that it is a ordinary text to instruct English to the children since we made it like that or in the event that they attempt to extract the original message, it requires a huge measure of computational time.

2.2] C Y. Zhou *et al*

According to security concern, some encryption and decryption algorithms are working behind private data like DES, 3DES, AES and Blowfish. In this paper from the outset new cryptography (Encryption and Decryption) algorithm has been created and new cryptography (Encryption and Decryption) algorithm has been analyzed by utilizing a few segments like throughput of key generation, to produce Encryption text and to produce Decryption text. On the off chance that any brute force attacks are applied on this algorithm, how much security is given by this algorithm is incorporated. In this algorithm some arithmetic and logical mathematical activities are performed.

3] PROBLEM DEFINTION:

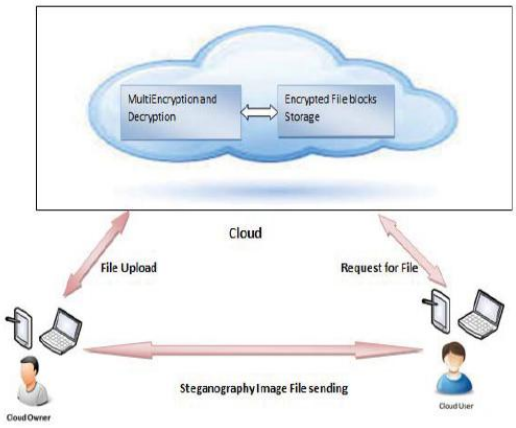
The proposed techniques for data sharing on a cloud involve less security and more time consumption. The issue arises when multi-user activity occurs. As we can say the deliver key to receivers into multi uses application. The existing algorithms require low delay for data encode decode but it provides low security. The main disadvantage of these techniques, it consumes more time for converting into text as it works on a single byte at a time. The usage of single symmetric key may face low performance and high security issues.

4] PROPOSED APPROACH:

Cloud computing techniques have been booming in the present days. To share, store, retrieve data with at most security and no time lapse. Many strategies have been introduced to cope up the issues facing by the cloud computing. Cryptography and steganography are amongst those which have been introduced. And these strategies follow AES, BLOWFISH, etc algorithms with secret keys to upload data on cloud. The main and crucial role of these algorithms is data integrity, security, confidentiality and for data encodes and decode. A blowfish algorithm's is main purpose is to produce high data confidentiality, and use

single key, need less amount of time for encode and decode.

5] SYSTEM ARCHITECTURE:



6] PROPOSED METHODOLOGY:

6.1] Cloud Server

The Cloud server manages which is to give data storage service to the Data Owners.

Data owners encode their data files and store them in the Server for imparting to data customers.

To get to the mutual data files, data consumers download encoded data files of their interest from the Server and afterward Server will decrypt them.

The server will produce the aggregate key if the end user demands for file approval to access and performs the accompanying tasks, for example, View all User Files, Give privileges to user ,View Search Transaction, View all aggressors ,View all End Users, View all Data Owners, Create Index on searched data and give every single related data related to corresponding keyword, View all android users

6.2] END User

The user can just access the data file with the secret key. The user can search the file for a specified keyword.

The data which matches for a specific keyword will be indexed in the cloud server and afterward reaction to the end user.

6.3] Data owner

The data provider transfers their encoded data in the Cloud server.

For the security reason the data owner encodes the data file and afterward store in the server.

The Data owner can have equipped for controlling the encoded data file and plays out the accompanying tasks Browse and enc and Uploads files, Grant Permission to consumer / End user

6.3] Android User

In future we can easily use this application.
This application user needs to introduce in a mobile. Before using this application user should enlist. After enrollment he ought to login by using approved user name and password.

After login successful he will do a few tasks, for example, searching keyword in the cloud server to discover KNN data and survey cloud attackers in the android mobiles.

7] ALGORITHM:

7.1] Hybrid algorithms:

Step 1: first AES algorithm is applied on file after that Blowfish algorithm is applied on encrypted data. Reverse process is followed for decryption. After applying keys that file covert into encoded form and stored on cloud server.

Step 2: blowfish algorithm is block level encryption algorithm.

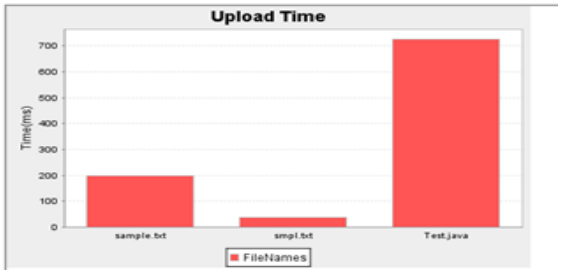
Step 3: AES, RC6, Blowfish and BRA algorithms are used for block wise security to data.

7.2] Steganography:

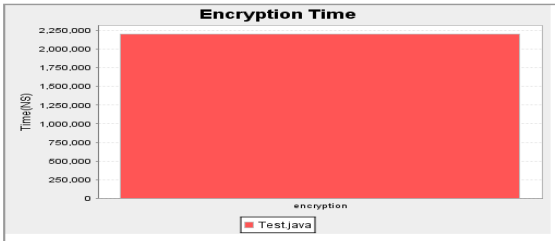
Hide key data into cover image using LSB technique.

After adding text into text cover file it looks like normal text file. If text file found by illegitimate user than also cannot get sensitive data.

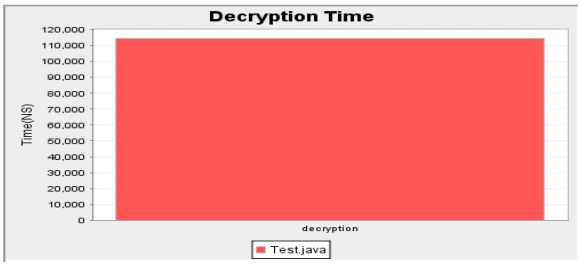
8] RESULTS:



The above graph shows that upload time. X-axis is file names, Y-axis is time(ms). It calculate the file uploaded time.



The above graph shows that encryption time for upload file. . X-axis is file names, Y-axis is time(ms).



The above graph shows that decryption time for upload file. X-axis is file names, Y-axis is time(ms).

9] CONCLUSION:

Cloud storage issues are solved using cryptography and steganogarphy strategies.

Block wise Data security is accomplished using AES, RC6, Blowfish and BRA algorithms. Key data security is cultivated using LSB technique.

10] EXTENSION WORK:

Data integrity is cultivated using SHA1 hash algorithm. Low delay parameter is accomplished using multithreading procedure. With the assistance of proposed security mechanism data integrity, high security, low deferral, validation and privacy boundaries are accomplished. Proposed Text file encryption need 17% to 20% less time as contrast with AES algorithm. For AES text decryption needs 15% to 17% most extreme time as contrast with proposed system. In Blowfish for encryption need 12% to 15% maximum time as contrast with proposed hybrid algorithm. Text file decryption using hybrid algorithm needs 10%

to 12% less time regarding Blowfish algorithm. In future, attempt to achieve high level security utilizing hybridization of public key cryptography algorithms.

11] REFERENCES:

[1] 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.

[2] Abu Marjan, Palash Uddin, "Developing Efficient Solution to Data 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 Architecture for the Advanced Encryption Standard Algorithm" IEEE,International Symposium on Design and Diagnostics of Electronic Circuits & Systems, pages 167- 170,April 2014.

[5] M. Nagle, D. Nilesh, "The New Cryptography Algorithm with High Throughput",IEEE, ICCCI ,pages 1-5,January 2014.

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

[7] N. Sharma ,A.Hasan, "A New Method Towards Encryption Schemes (Name-Based-Encryption Algorithm)",IEEE, International Conference on Reliability, Optimization and Data Technology,pages 310-313,Feb 2014.

[8] 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 Data Technology,pages 310-313,Feb 2014.

[9] 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.

[10] 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.

Profiles:

Mrs. G. Umasowjanya is a student of Pragati Engineering College, Surampalem. Presently she is pursuing her M.Tech [Computer Science &

Engineering] from this college and she received her B.Tech from Pragati Engineering College, affiliated to JNT University, Kakinada in the year 2010. Her area of interest includes Object oriented Programming languages, all current trends and techniques in Computer Science.

Mrs. G. Kumari is working as an Assistant Professor in department of Computer Science and Engineering, Pragati Engineering College. She acquired her Bachelor of Technology, Masters in computer science and engineering. She has 13 years of teaching experience. Her areas of interest include Network Security, Data mining and Mobile Networks.