International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

CRYPTOGRAPHY IN CLOUD COMPUTING

Ganashree R,

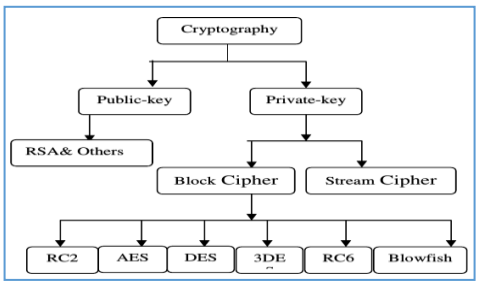
ABSTRACT

This paper mainly aims at protecting the data from unauthorized users by splitting the data into several parts and storing it in the cloud to ensure data integrity, confidentiality of and availability of data. The software is provided at low cost, as many organizations and IT industries have increased the use of cloud. Cloud computing has its own advantages in terms of accessibility of data and low cost.

Securing the data from unauthorized users is the main aim of cloud storage. Users usually store the sensitive data with cloud storage which are not trusted. It's still a challenging issue to secure the sensitive data from the unauthorized users. Our approach is to ensure privacy of the data stored in the cloud by using AES, DES and RC2 algorithm.

1. INTRODUCTION

Cryptography is the process of converting the readable form of data into non readable form to secure the data from the unauthorized users. The main aim of cryptography is to protect the data from the third party. Two types of algorithms are used to secure the data from the unauthorized users. They are symmetric key based algorithm and asymmetric key based algorithm.



As some confidential and sensitive data is stored in cloud computing environment by the users, securing the data plays a major role. Hence the management of data must be completely trusted. The data must be protected from the software which is malicious. Data confidentiality, availability and integrity in cloud are provided to ensure data security. When unauthorized users access the data, it results in loss of data confidentiality. When the cloud services fail to protect the data from unauthorized users, data integrity and availability are affected.

The services provided by cloud are not restricted to any domain. All the authorized users are allowed to access the data whenever required. This project provides the database which stores all the login credentials which are required by the users.

The data stored in the cloud can be accessed from anywhere with the help of the internet. The users of the cloud can access the data from the cloud by providing login credentials. The security for the data stored in the server is provided by the cloud.

2. PROBLEM STATEMENT

User stores the data in the cloud which is open to several threats. The single point of failure which is the first threat which affects the data availability where the server crashes or fails its functionality. If the server runs out of its service, then the data availability is affected.

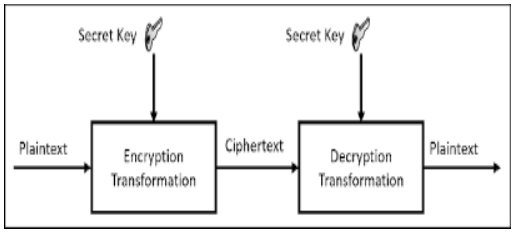
Data integrity is our second threat. The data can be altered only by an authorized person which is called as data integrity. Unauthorized person cannot alter the data or the text which is stored in the cloud. Therefore, the user of the cloud cannot entirely depend on the cloud service providers.

Security is an important key for the data which is transmitted either through wired or wireless network. The data cannot be stored on Cloud without any security. It should be provided with security, which is a real challenge. The data must be reconstructed using a secret key to prevent loss of data.

As cloud is a multi-user environment, users fear in loss of data and confidentiality of data. Cloud is also a third-party service where there is a risk of data being mishandled. It is not said to be secure, when the business sensitive data is being handled by third party service providers. External risks which may include malicious hacks or compromises of user accounts may result in data leakage. To avoid data loss and to protect data confidentiality, we use strong passwords and file encryption methods.

3. FRAMEWORK

a. Symmetric key cryptography



Symmetric key cryptography is a type of data encryption method where the sender who sends the data and the receiver who receives the data share the same key for transferring the data from one end to another end. The only encryption method known to the public until June 1976 was symmetric key cryptography.

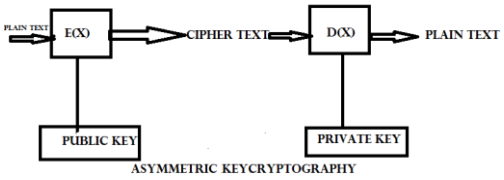
Stream ciphers and block ciphers are the two types of symmetric ciphers.They are used in symmetric key cryptography.

The function of Block cipher is to convert plain text into cipher text. Stream cipher converts cipher into text into plain text.

Block cipher designs such as the data encryption standard and advanced encryption standard which are designated cryptography standards by the US Government.

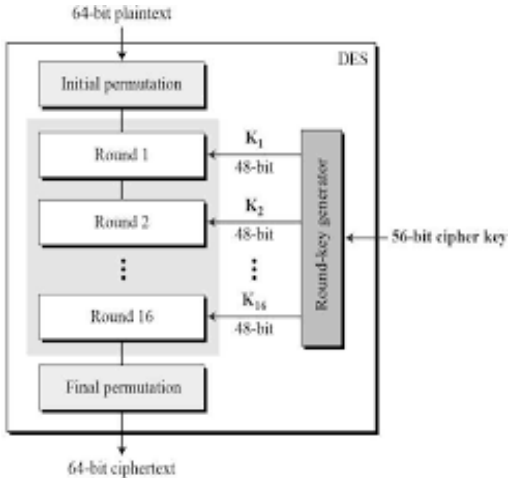
b. Asymmetric key cryptography

Asymmetric cryptography which is known as open key cryptography. Encryption and decoding of the text are finished involving two keys in topsy-turvy key cryptography. The keys utilized in this method are called private and public keys.
Shipper encodes the message utilizing a public key and the confidential key is utilized by the collector to unscramble the message.



ASYMMETRIC KEYCRYPTOGRAPHY

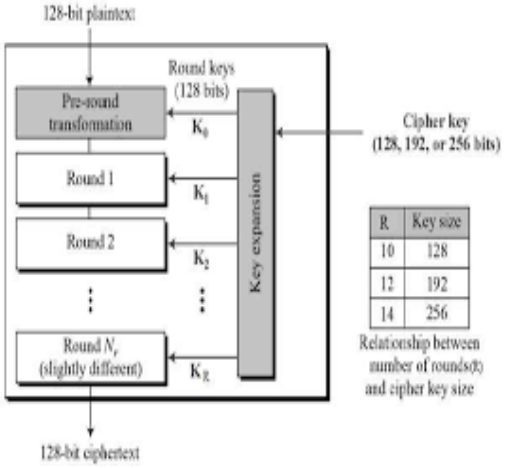
4. DATA ENCRYPTION STANDARD



DES is one of the most powerful attacks in cryptography where 64 bits of plain text are then converted into 48 bits of cipher text. DES algorithm uses a single key for encryption and decryption as it a symmetric key algorithm to protect the access of data from unauthorized users.DES calculation is a block figure as it takes just fixed length of line of plain text and afterward changes over it into figure text. The key usually consists of 64 bits but the algorithm uses only 56. 8 bits which are remaining are used to check the parity.

5. ADVANCED ENCRYPTION STANDARD

It is most used symmetric algorithm. DES is six times slower than AES.DES was replaced by AES as its key size was too small. AES functions are based on bytes. Hence 128 bits are considered as 16 bytes of plain text and then it is arranged in the form of rows and columns in the form of matrix. There are 2 different key lengths in AES they are 128,192 and 256 bits. Each round in AES consists of four sub processes.



a. **SUB SUBSTITUTION**
The info is given as 16 bytes, which is subbed involving the decent table given in the plan. The outcome will be as a framework which comprises of four lines and four sections.

b. SHIFT ROWS
Each column in the grid should be moved to its left side. Shifts are completed as referenced beneath
First column in the grid isn't moved.
Substitute column is moved left by one position.
Third column is moved by two situations to its left side.
Shift fourth column by three positions.
The outcome in the new network which has 16 bytes.

c. MIX COLOUM
Every segment of four bytes is changed over utilizing an exact capacity. It takes the contribution of 4 bytes and furthermore returns the new 4 bytes which will supplant the first segment..

d. ADDROUND KEY

The lattice which comprises of 16 bytes are currently thought to be as 128 pieces and are presently XORed utilizing the round key.
The result is figure text in the event that there's a last round

6. DECRYPTION

To get the information from unapproved clients, the code text which is in non-meaningful structure is changed over into plain text which is in coherent structure is called decoding. Decoding is for the most part finished at the gets end. The correspondence which is interpreted is unraveled utilizing private key or mystery key. Each round comprises of four cycles which are directed in the turned around request.
• Add round key.
• Blend section.
• Shift lines.
• Byte substitution.

7. CONCLUSION

The owner has zero command over the security to store and access the information. The information is to be protected from unapproved clients and the approved clients should be proficient to get to the information which is the primary plan of cryptography. Encryption calculation which is utilized to encode the information is one of the principal benefits to improve execution during encryption and decoding process. This approach to putting away and entering the information forestalls information misfortune and results in elite execution.

REFERENCES

[1] "J. RIVES CHILDS", "*General Solution of the ADFGVX Cipher System"*, California, 2001.

[2] "C. E. SHANNON", "Communication Theory of Secrecy Systems", *Bell Systems Technical Journal*.

[3] "D. R. Hankerson", "D. G. Hoffman", "D. A. Leonard", "C. C. Lindner", "K. T. Phelps", "C. A. Rodger", and "J. R. Well". "Coding Theory and Cryptography, the Essentials", "Marcel Dekker", New York, 2000

[4] "M. Miller. Symmetrische Verschlüsselungsverfahren". Teubner, Stuttgart, 2003.