International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 09 | Sep 2020 www.irjet.net p-ISSN: 2395-0072

Data security in Cloud by Dual Layer Encryption

Mr. Himanshu Taiwade[1], Miss. Pragati Meshram[2], Miss. Janhavi Dixit[3], Mr. Devendra Raut[4], Mr. Zeeshan Sabir[5]

[1]Professor, Dept. Computer Science and Engineering, Priyadarshini Institute of Engineering and Technology, Nagpur, India
[2-5]Dept.Computer Science and Engineering, Priyadarshini Institute of Engineering and Technology, Nagpur,India

---

ABSTRACT: *The use of internet and remote servers for data sharing and transferring has created a boom in the field of social networking. However, user data can be accessed and manipulated by any malicious users over the internet service. Regardless of flexibility of data and accessing of applications, there are many concerns about how to achieve a reliable environment that protects application and data in the cloud from malicious intruders. This paper proposes a new generation of dual layer encryption using key cryptography for making a model which is secure and safe. The main approach of this paper is to ensure security in the cloud. The aim of this paper is to suggest the new secure system named as dual layer of encryption. In this system Advance Encryption Standard (AES) is going to be the first layer of encryption which is already a secure algorithm, also there is an extra added layer of Rabbit Algorithm which is a secure and very fast encryption. Every day user create and transfer a large volume of data with other networks. It has been notice that there is no major attack on AES yet. AES is used by many of the IT industries and organizations as it has been proved that the use of AES is safer in there implementation . This scheme makes full use of the dynamic processing skill of cloud computing along with ensuring cloud data privacy and security too.*

1. INTRODUCTION:

In the cloud, the data is shared between the server cases client. High speed is the basic need of any service, cryptography offers various options to secure and safeguard the transfer of information from the cloud. Data encryption is also called a security method where data is encrypted and decrypted by a user with the right encryption key. Encrypted data appears distorted or unreadable to a person who is accessing it without prior permission. Now there are two sort of encryption. The first type of encryption is called symmetric cryptography or shared secret encryption. This encryption uses a secret key called a key, to convert the data into respective cypher data. The person at the receiving end needs the key to unlock the data. By changing the key, you can change the results of the encryption. It took a few years, but finally DiffiePartnered with Martin Hellman and Ralph Merkle came up with a new system called **public key encryption** (PKE), also known as **asymmetric cryptography**. It make use of encryption that splits the key into two smaller keys. One of them is made public and one is kept private. The use can be encrypt the message with the recipient's public key.. Recipient can then decrypt the message with their private key and vice versa. The important difference here is that you don't need to have someone's private key to send him or her a reliable and secure message. This process allows two users to communicate securely and safely without any prior exchange of keys and information.

2. LITERATURE SERVEY :

In this paper discuss about dual layer security technique which used stenography and cryptography for the confidential data transfer. The data is send by using first S-DES encryption algorithm and then that data is enclosed within a image enclosed within an image. Dissimilar to other procedure this type of method doesn't send cryptographic key separately [1]. The use of dual layer encryption give surety for high security and information. Dual layer enryption is a good technique for securing the data in cloud.[2].The procedure proposed here used the combination of cryptography and image steganography the cryptography technique is used for the encrypted secret message is based on content encryption algorithm and the steganography technique are used LSB and raster scan technique.[3].The paper discussed the multiple technology and technique and their problem associated with their security. The paper has classification for the published technique, which focus on cryptography and steganography technique as well as a combination of both the techniques. [4]In this paper discuss a two level of security on data. First level is a public key cryptography and the second level the message is encrypted and stored in a series of shuffled and identical image. [5].In this paper new work is discussed which is multi-layer encryption which is based on the Advanced Encryption standard (AES) and Rivest-Shamir-Adleman (RSA) algorithm which help to provide hi security and privacy of data on cloud[6]. In this paper discussed which is extended AES algorithm with custom configurable encryption.The added layer of security is based on the caesar cipher encryption algorithm[7].

3. PROPOSED METHOD :

Nowadays AES is likely to be used as the most effective and powerful algorithm But we presumed that in some cases AES is not enough for security, So for more security purposes we have experimented AES with Rabbit algorithm which is also a symmetric algorithm as AES but

stream cipher in nature as an additional security for data transmission.

As mentioned in the abstract ,the paper proposed an extra added layer of encryption which provides more security and makes hard to decrypt the data. Here we have used two different layers of cryptographic algorithms, one layer is a stream cipher and the other one is a block cipher algorithm. Both the algorithms are symmetric in nature, the algorithms we have worked on are AES and Rabbit of 256 and 128 bits respectively.

The main idea is twice encryption of data before sending it to the cloud. The basic use of this technique is to secure the data from malicious attackers while transferring the data from sender to cloud storage.

Combination of AES and Rabbit:-

- ***Encryption using AES-256:*** This is the first layer of encryption, In this paper work AES algorithm plays an important role. Firstly by using the AES-256 encryption algorithm we encrypt the original data and convert it into cipher text.

Operation of AES:AES is considered the most powerful encryption algorithm. Interesting about AES is that it performs the computation on bytes, for example plaintext of 128 bits converts into 16 bytes. Depending on the length of the key size it takes rounds. Plaintext uses bytes and arranges that in matrix in columns and in rows. In the first layer we have used the AES-256 bit encryption algorithm. 256 bits of AES encryption uses 14 rounds and converts it to 32 bytes. In rounds, transformation of each column is done by using a mathematical

functions – 1. Sub-bytes

2. Shift rows
3. Mix column
4. Add round key

Sub bytes:- The very first step of AES algorithm is sub-bytes . The original message here is converted to cipher text. Here the original message is plain text which is converted to hexadecimal or can be converted to binary. Next step to chunk the data into blocks of equal size.

Shift row:-This is the next step performed over substituted data. Take each row and shift it by 1 hexadecimal place except 1st row.

Mix column:-Here we take columns of data and then we multiply it by a specific Matrix.

Add round key:-In the first round we take a block of data and add a key to it, the key is like a password. We get a block of ciphertext as a result which is of the same size. Then we will have a key remainder, after performance key addition to block and take key and combine it to the next block. Every time a new key gets added to the new block for more security.

The output completely replaces the previous column and results into new output in every round. At the last round we get cipher text. While in the Decryption process the procedure just adopts the reverse manner of the encryption algorithm. Algorithms for decryption need to be implemented separately as they are very similar to encryption processes.

- ***Rabbit algorithm:*** rabbit algorithm basically is a stream cipher algorithm. We used this algorithm in the second layer. We take AES cipher text as input and convert into another cipher text using rabbit algorithm. Rabbit algorithm make use of same key for encryption and decryption. It uses a key size of 28 bit whereas initialization vector (IV) of 64 bit. 128 bits are encrypted by per iteration. Strength of cipher text depends upon mixing functions in consecutive iterations. Mixing function performed arithmetical operation or g function or ARX (add rotate xor) operation and 2^{32} modulo of addition.

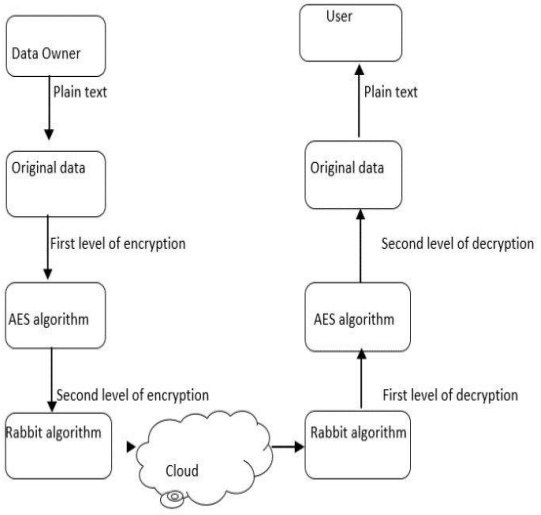

Fig 1. Dual layer encryption / decryption

Rabbit algorithm here takes the cipher text from AES as input and converts it into 128 bit text if AES cipher text is of 256 bit or 192 bits. Rabbit is a stream cipher algorithm which works only on 128 bit. It increases the high speed performance of algorithms.

Rabbit algorithm is a stream cipher algorithm, it is mainly designed to be faster than commonly used algorithms.

Working:

a) Key setup scheme :-

The algorithm was initialized by expanding the 128-bit key into eight states variables and eight counters. The state and variable are initialized from the sub-keys, this system iterates four times to decrease correlation between key bits and state variable bits.

Counter variable reinitialize according

b) IV Setup Scheme: Suppose the internal state after the key setup scheme after formation is master state, and let copy of this master state be modified according to the IV scheme. 64 bits IV are XOR with o counter states of 256 bits. This scheme modifies the counter state as a function of the IV.

c) Next-state Function: The main part of the rabbit algorithm is the iteration of the system which is by the following equations:

x0,p+1 = h0,p + (h7,p <<< 16) + (h6,p <<< 16)

x1,p+1 = h1,p + (h0,p <<< 8) + h7,p

x2,p+1 = h2,p + (h1,p <<< 16) + (h0,p <<< 16)

x3,p+1 = h3,p + (h2,p <<< 8) + h1,p

x4,p+1 = h4,p + (h3,p <<< 16) + (h2,p <<< 16)

x5,p+1 = h5,p + (h4,p <<< 8) + h3,p

x6,p+1 = h6,p + (h5,p <<< 16) + (h4,p <<< 16)

x7,p+1 = h7,p + (h6,p <<< 8) + h5,p

hq,p = ((xq,p + cq,p+1) 2 ⊕ ((xq,p + cq,p+1) 2 >> 32)) mod 2 to the power32

d) Counter System:

The dynamics of the counters is explained as follows:

m0,p+1 = m0,p + k0 + Ø7,p mod 2 to the power32

m1,p+1 = m1,p + k1 + Ø0,p+1 mod2 to the power32

m2,p+1 = m2,p + k2 + Ø1,p+1 mod 2 to the power32

m3,p+1 = m3,p + k3 + Ø2,p+1 mod 2 to the power32

m4,p+1 = m4,p + k4 + Ø3,p+1 mod 2 to the power32

m5,p+1 = m5,p + k5 + Ø4,p+1 mod 2 to the power32

m6,p+1 = m6,p + k6 + Ø5,p+1 mod 2 to the power32

m7,p+1 = m7,p + k7 + Ø6,p+1 mod 2 to the power32

furthermore, the kq constants are defined as:

k0 = 0x4N34N34N

k1 = 0xN34N34N3

k2 = 0x34N34N34

k3 = 0x4N34N34N

k4 = 0xN34N34N3

k5 = 0x34N34N34

k6 = 0x4N34N34N

k7 = 0xN34N34N3

e) Extraction Scheme:

After each iteration the output is extracted as follows:

tp [15..0] =x0,p[15..0] ⊕ x5,p[31..16] tp [31..16] =x0,p[31..16] ⊕ x3,p[15..0]

tp [17..32] =x2,p[15..0] ⊕ x7,p[31..16] tp [63..48] =x2,p[31..16] ⊕ x5,p[15..0]

tp [79..64] =x4,p[15..0] ⊕ x1,p[31..16] tp [95..80] =x4,p[31..16] ⊕ x7,p[15..0]

tp [111..96] =x6,p[15..0] ⊕ x3,p[31..16] tp [127..112]=x6,p[31..16]⊕ x1,p[15..0]

where tp is the 128-bit key stream block at iteration . The extracted bits are XORed with the cipher texts which comes from the AES algorithm and output will be encrypted cipher text and decryption vice versa after the rabbit algorithm we get double encrypted data**.**

4. CONCLUSION:

Increased use of cloud computing for storing data certainly raises the security concern of cloud security. Data available in the cloud can be at risk if not protected in a justified manner. Although cloud provides prevention by their own security modules discussed in this paper which discusses the risks and security threats to data in the cloud and gives an overview of dual layer data encryption techniques which will provide us better security. One of the major aspects of this paper is data security and solutions to various threats in cloud computing. Further this paper discusses the dual layer encryption technique which is efficient for encrypting the data in the cloud. The study provides us with an overview of Rabbit algorithm and AES algorithm which can be efficiently used for encrypting the data in the cloud.

5. REFERENCES :

[1] Biswajit Datta , Akash Roy , Romit Dutta , Samir Kumar Bandyopadhyay "Secure Communication through Double Layer Security with Efficient Key Transmission" 2018 International Conference on Information Technology (ICIT) (IEEE)

[2] M.Subbulakshmi, Dr.D.Usha "Double Layer Encryption Algorithm Key Cryptography for Secure Data Sharing in Cloud" International Journal of Scientific & Engineering Research Volume 9, Issue 5, May-2018

[3] Jyotsna, Janmejai Kumar ,Shivani Chauhan, Amit Doegar "Multiple layer Text security using Variable block size Cryptography and Image Steganography" 3 rd IEEE International Conference on "Computational Intelligence and Communication Technology" (IEEE-CICT 2017)

[4] Geetha D Devanagavi[2] ,,Gahan A V "A Empirical Study of Security Issues In Encryption Techniques" International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 5 (2019)

[5] Santhosha1, Ashok Kumar1 " Two layer Security for data storage in cloud " 2015 1st International conference on futuristic trend in computational analysis and knowledge management (ABLAZE 2015)

[6] K.Thippeswamy , Naveen N "Security and Privacy Challenges Using Multi-Layer Encryption Approaches In Cloud Computing Environments" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-8 June, 2019

[7] Shreyam Dasgupta, Pritish Das " Extended AES Algorithm With Custom Encryption for Goverment-level Classified Messages" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075,Volume-8,June,2019