International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Implementing Information Security Mechanism Over Cloud Network

Thejas Bharathan, Santhosh Kumar B J

Abstract— The security parts of distributed computing, particularly the security of information, turn out to be increasingly essential. It is important to build up another component to verify the information in the cloud. Cryptographic based symmetric key cryptosystems helps to provide an efficient way to protect information. Enhanced symmetric key cryptosystem AES algorithm has been proposed for securing the data and safely storing to the cloud. This paper is to provide an overall security to the files which are in the cloud so the encrypted file can be retrieved at any time from the cloud. The paper also aims to introduce the mechanism use to secure cloud computing applications as well as to compare some existing algorithm like RSA and AES with an enhanced AES algorithm and to prove that the proposed algorithm is more effective than the other two algorithms. The encryption speed of the algorithms is graphically represented in the paper.

Keywords —RSA, AES. Enhanced AES, and AWS

I. INTRODUCTION

A personal computer framework or accumulation of frameworks are the medium which grants pcs to trade information. Systems administration is the accumulation of frameworks associated each other to play out a particular undertaking. The frameworks are associated through different links like optical fiber, turned pair links and so forth. To characterize the engineering of any system numerous topologies are accessible, for example ring, star, transport and so forth. There are two kinds of systems administration, association situated and connectionless where the association arranged system administration builds up an association before sending the information, in connectionless systems administration there is no need of association. Cryptography is a region which give a few strategies to accomplish protection of the files incorporates privacy, verify action, security, respectability.it is important to secure the information which is exchanging through web or any medium. The information may assaulted by outsider.to guarantee the uprightness we have a few procedures like RSA, AES. The proposed method is based on AES algorithm model, switch, portal these are the equipment gadgets used to interface the pcs in organize. The owner can't guarantee its respectability while trading the information through medium. The third person may take the file, alter the file or they can obliterate it. Amazon simple storage service (amazon s3) is an item stockpiling administration that offers industry-driving versatility, information accessibility, security and execution. This implies clients everything being equal and ventures can utilize it to store and ensure any measure of information for a scope of utilization cases. Modern cryptography focuses on the following four objectives:

- *Confidentiality:* anyone can unconsciously understand the information.
- *Integrity:* information cannot be altered in accumulating or sending between the owner and the receiver without detecting a change.
- *Authentication:* The sender and recipient can confirm the identity of the other party and the source or destination of the image

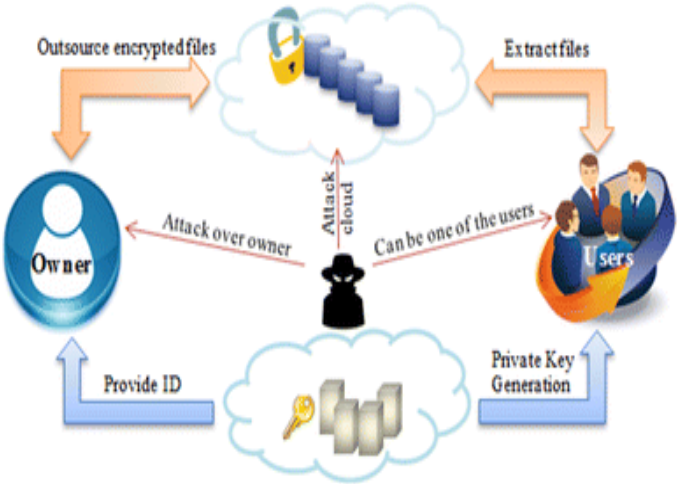

Fig1.cloud security

The files in the cloud can be attacked at any time by the intruder. Cloud security is very essential in the modern world. The above diagram shows different attack scenarios where one can attack the cloud. once the intruder come to know the key or particular id his/her work will be so easy, there are different crypto mechanisms in the world they are of 2 kinds, symmetric and asymmetric, in symmetric crypto mechanism, for encryption and decryption one key is used where as in asymmetric crypto mechanism different keys are used for encryption and decryption.. Symmetric key crypto mechanism is used in my proposed methodology. AWS cloud storage is used in my work. For storing the files and retrieving the data at any time. AWS cloud storage provider is more user friendly than any other cloud.
The paper includes contents in the following way.

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
Thejas Bharathan*, Department of Computer Science, Amrita School of Arts and Sciences, Amrita Vishwa Vidyapeetham, Mysuru, India
Santhosh Kumar B J, Department of Computer Science, Amrita School of Arts and Sciences, Amrita Vishwa Vidyapeetham, Mysuru, India

Section II literature survey. Section III deals with the existing methodologies. Section IV is done with the proposed methodology. Section V is all about experimental results and at last section VI and VII are of conclusion and future work.

II. LITERATURE SURVEY

Abha sachdev et.al [1] used AES algorithm for cloud computing the data are being encrypted before it is stored. Data confidentiality and security is ensured here. In AES, 128 bit keys are used to encrypt. 192 and 256 bit keys are also used in AES. Once the file is stored in the cloud it is safe for user to get the data at any time.

Boukhatem Mohammed belkaid et.al [2] encrypted meteosat images are encrypted using AES and RSA algorithm. Cryptographic analysis and various algorithms are performed and the result are reported in this paper. Experimental results shows that the pixels values of the image are evenly distributed, widely used for secure capacity and transmission of secret message pictures over the web or any common system conditions.

Dr. Prerna Mahajan et.al [3] the file security of AES, des and RSA algorithms are studied. Three encryption technologies such as AES, DES and RSA algorithms are implemented and encryption technology is compared based on the stimulus time analysis during encryption and decryption on the text files. Reasoned that the AES calculation devours minimal measure of encryption time and RSA expends the longest encryption time.

Eman salim Ibrahim harba [4] joined AES, RSA and HMAC for secure information encryption. A technique was proposes to ensure information exchanging. AES calculation used to encode documents, RSA used to scramble AES secret phase and HMAC to scramble symmetric secret key and information to guarantee a safe transmission between server/customer or customer/customer structure make it difficult to find regular assaulted techniques. The general encryption run is basic and quick with low computational prerequisites and gives high framework security.

Fausto meneses et.al [5] worked on RSA encryption calculation streamlining to improve execution and security dimension of system message. Security achieved by optimized RSA algorithm, integrity and availability of information they are planning to do this algorithm in DLL platform in future.

Nasrin khanezaei et.al [6] finished the distributed computing administration structure dependent on RSA and AES calculations. Data is shared with the users in the cloud network in conjunction with RSA and AES algorithms. Generating asymmetric key is time consuming. For large files, it is very difficult to encrypt using an asymmetric encryption algorithm like RSA.

Kriangsiri malasri et.al [7] worked on medical sensor network security. For confidentiality and integrity symmetric encryption mechanism is used for verifying data source a two-tier authentication scheme is used. Describe three security mechanisms in SNAP, communication between nodes and base station of various attack is emphasized.

M.zeghid et.al [8] proposed image encryption technique using modified AES algorithm. Modified TSA algorithm is a symmetric mechanism were secure data encryption is enabled. The encrypted image is less untellable than the previous one.

Manika sharma et.al [9] the visual image is encrypted using the RSA algorithm. Use visual encryption technology, the mystery picture is partitioned in to ‘ n’ number and shared in to the system the drawback of these plans is that just a single, lot of mystery messages can be inserted, so as to share an expensive number of mystery messages, a few offers to be created and keys must be send safely. A visual cryptography plot is proposed in which the nature of the unscrambled picture is improved when shading blunder dissemination systems are utilized.

Parsi kalpana et.al [10] information security in cloud processed is done using RSA calculation. There is no information close to the cloud client. Moreover they executed RSA calculation to guarantee security. Scramble information utilizing the RSA calculation to give security with the goal that just significant clients can get to it.

Rachna Arora et.al [11] use encryption calculations to think about secure client information in distributed computing. The security issue, mechanism and challenges faced by cloud service providers in cloud engineering and the metaphorical research of various security algorithms. The advantages of cloud computing traditional calculation include: agility, reduced entry cost, device independence, location and scalability. The main disadvantages is that the danger of intruders in the cloud. The disappointments of cloud administrations have been emphatically viewed by the organization.

Shahzadi Farah et.al [12] led test think on the execution assessment of lop-sided cryptographic calculations. diverse analysis have been performed to think about the encryption time ,decoding time , memory use and throughput of variable content record and private key sizes for these calculations .RSA, ElGammal, pallier implement compare various text file size .RSA performs superior to ElGammal and pallier regarding encryption time, and elgammal displays preferred execution over RSA and pallier in unscrambling.

Suchita tayde et.al[13] the AES algorithm is used in android phone application for the file encryption and decryption ,allowing users to run this application to keep running on android stage to scramble files before they are passed over the network. It is used for a wide scope of archive encryption. Example content, docx, and pdf and picture encryption are encrypted using this. The AES calculation is utilized for encryption and decoding. This articles demonstrate the successful implementation of file and image encryption and decryption.

William puech et.al [14] done a new medical image security transfer encrypting watermark method. Another strategy joining image encryption and water marking technology for secure transmission. A method of combining encrypted and watermarking is proposed for the image security transmission using encryption algorithm, secret key and public key.

Santhosh Kumar BJ et.al [15] compared RSA and AES algorithm for different medical images, by the way of comparison it comes to know that the AES algorithm is more efficient than RSA algorithm for the set of data.

III. EXISTING METHODOLOGY

RSA algorithm

Step 1: selecting two prime numbers, take it as variable p, q.
Step 2: calculate n=p*q and φ = (p-1) (q-1)
Step 3: find 'e' where 1<e< where' e 'is moderately prime to φ
Step 4: calculate unique integer'd'.1<d< φ
Step 5: use encryption formula

$$C=M^e \bmod n$$

Step 6: use decryption formula

$$M=C^d \bmod n$$

RSA calculation is uneven cryptography calculations. Here uneven implies that the same algorithm deals with two distinctive keys for example open key and private key. By the name itself we can understand that open key is shared with everyone and the private key is owned by the one who want to decrypt the message. In RSA algorithm the public and private keys are obtained by factorizing two large prime numbers. Multiplying two large prime numbers becomes a huge number so the intruder can't easily compromise the key. This is the main strength of RSA.

AES Algorithm

1. Derive the arrangement of round keys from figure key.
2. Initialize the state cluster with the square information (plain content).
3. Add the underlying round key to the beginning state exhibit.
4. Perform nine rounds of state control
5. Perform the tenth and last round of state control
6. Copy the last state exhibit out as the encoded information (figure content).

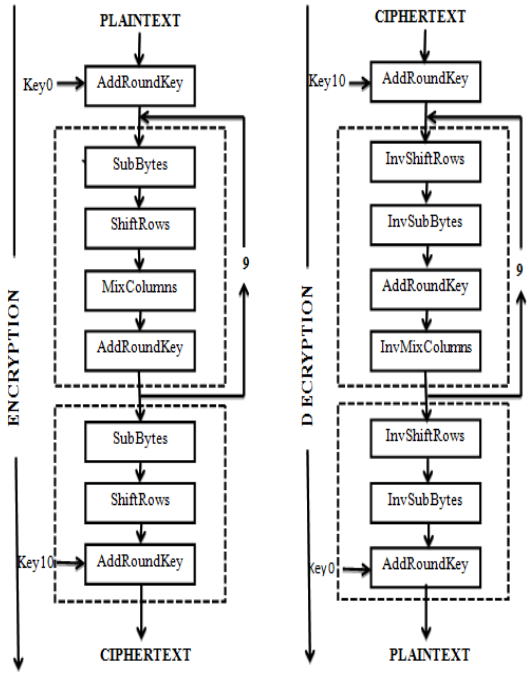

Fig2. AES encryption and decryption

AES is an iterative instead of feistel figure. It depends on substitution.it includes a progression of connected activities, some of which include supplanting contributions by explicit yields(substitution)and others include rearranging bits around(stages). AES plays out the calculations on bytes as opposed to bits. Consequently AES treats the 128 bits of a plaintext obstruct as 16 bytes .these 16 bytes are organized in a matrix model. In contrast to DES, the quantity of rounds in AES is variable and relies upon the length of the key. AES utilizes 10 rounds for 128-piece keys, 12 rounds for 192-piece keys and 14 rounds for 256- piece keys. Every one of these rounds utilizes an alternate 128- piece round key, which is determined from the first AES key. The above figure shows the AES encryption and decryption process. As shown in the figure different steps are carried out continuously to encrypt the message. If the key is 128 bit then then 10 rounds are carried out.

IV. PROPOSED METHODOLOGY

Enhanced AES algorithm

1. P=5, is the number we want to factorize.
2. Y= arbitrary number, for example 1<y<n-1
3. Y is raised to the power contained in the register (each conceivable state) a while later divided by p. other activities taken place in 4 qubit register. The second register currently contains the super position results, assume y=2 which is larger than1 and lesser than 4.
4. In the event that we raise y to the forces of 4 qubit register, which is a limit of 5 and isolated by 5.what we see in the outcome is a rehashing arrangement of four numbers (1, 2, 4 and 8). We can certainly say then that f=4 which is succession when y=2 and p=5. The esteem y can be utilized to compute a conceivable factor with accompanying condition:

x= y f/2-1.

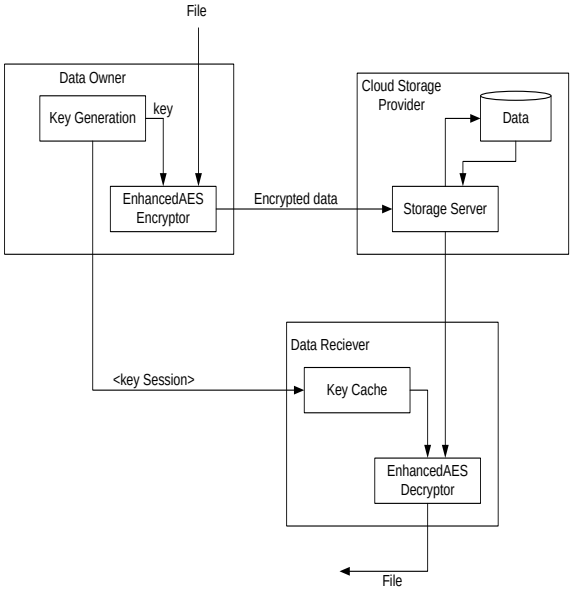

Fig2. Enhanced AES rough architecture

The file to be encrypted is split into five parts and the 128 bit key is distributed to each part, so that the encryption process will be more efficient than the existing algorithms. Figure 2 gives a rough architecture of the proposed methodology. The owner generates the key using enhanced AES encryptor, once the key is generated the file will be encrypted and stored in the cloud. Anyone can retrieve the data at any given time once the user have the decryption key

V. EXPERIMENTAL RESULTS

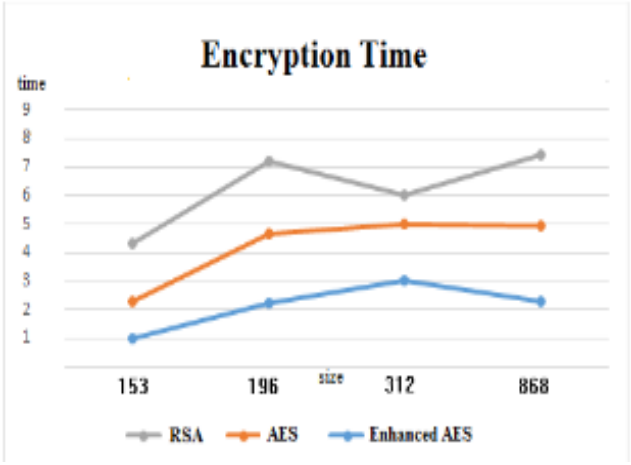

Fig3. Encryption time for images using 3 algorithms

Encryption time of images of different sizes are calculated using AES ,RSA and Enhanced AES algorithm. It shows that the enhanced AES algorithm is taking less time to encrypt the given files than other two existing algorithms namely RSA and AES algorithm.

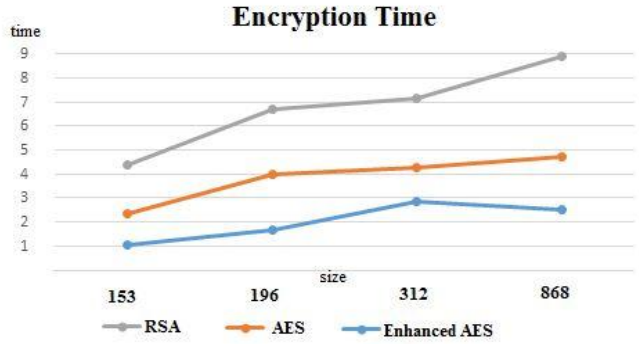

Fig4. Encryption time for text files using 3 algorithms

Encryption time of .txt files of various sizes are calculated with AES ,RSA and Enhanced AES algorithm,it shows that the enhanced AES algorithm is taking less time to encrypt the given files than other two existing algorithms namely RSA and AES algorithm.

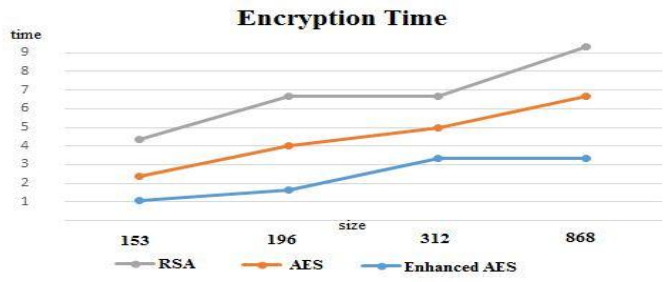

Fig5.encryption time for CSV files using 3 algorithms

Encryption time of CSV files of different sizes are calculated with AES ,RSA and Enhanced AES algorithm,it shows that the enhanced AES algorithm is taking less time to encrypt the given files than other two existing algorithms namely RSA and AES algorithm.

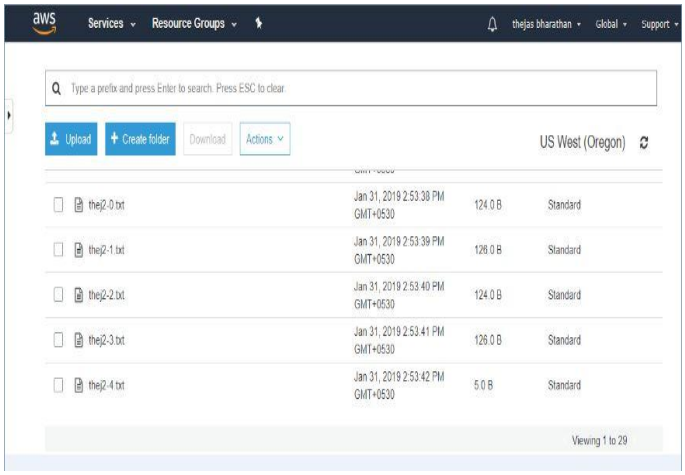

Fig4 files stored in AWS cloud

The data which are encrypted is stored in the AWS cloud. As the one data are encrypted part by part the files are stored part by part in the cloud. The user can retrieve the data at any time from the cloud . using the decryption key one can decrypt and get the original data.

VI. CONCLUSION

This paper addresses the comparison of three algorithms (RSA, AES, EnhancedAES).The comparisons is done with three different files (text, images, CSV). By comparing the three techniques used in the paper comes to the conclusion that the EnhancedAES algorithm is more efficient in both encryption and decryption for the three different data. The proposed algorithm is a symmetric crypto mechanism. By splitting the large file in to small parts and distributing the keys in to each part of the file and encrypting becomes more effective.

FUTURE WORK

Here we used text, CSV and image files as the input. These files are being encrypted and stored in the cloud In our future work video and live stream files can also be added for the same.

REFFERENCE

1. A. Sachdev, “Enhancing Cloud Computing Security using AES Algorithm,” vol. 67, no. 9, pp. 19–23, 2013.
2. M. I. Encryption, “Meteosat Images Encryption based on AES and RSA Algorithms,” vol. 6, no. 6, pp. 203–208, 2015.
3. P. Mahajan and A. Sachdeva, “A Study of Encryption Algorithms AES, DES and RSA for Security,” vol. 13, no. 15, 2013.
4. E. Salim and I. Harba, “Secure Data Encryption Through a Combination of,” vol. 7, no. 4, pp. 1781–1785, 2017.
5. F. Meneses *et al.*, “RSA Encryption Algorithm Optimization to Improve Performance and Security Level of Network Messages,” vol. 16, no. 8, 2016.
6. N. Khanezaei, “A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services,” no. December, pp. 12–14, 2014.
7. K. Malasri and L. Wang, “Addressing Security in Medical Sensor Networks ∗,” 2007.
8. M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, “A Modified AES Based Algorithm for Image Encryption,” vol. 1, no. 3, pp. 745–750, 2007.

9. M. Sharma and R. Saraswat, "Secure Visual Cryptography Technique for Color Images Using RSA Algorithm," vol. 2, no. 10, pp. 183–186, 2013.
10. P. Kalpana, "Data Security in Cloud Computing using RSA Algorithm," vol. 1, no. 4, pp. 143–146, 2012.
11. R. Arora and A. Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithms," vol. 3, no. 4, pp. 1922–1926, 2013.
12. S. Farah, M. Y. Javed, A. Shamim, and T. Nawaz, "An experimental study on Performance Evaluation of Asymmetric Encryption Algorithms 2 Literature Review," pp. 121–124.
13. S. Tayde, A. Prof, and S. Siledar, "File Encryption , Decryption Using AES Algorithm in Android Phone," vol. 5, no. 5, pp. 550–554, 2015.
14. W. Puech *et al.*, "A New Crypto-Watermarking Method for Medical Images Safe Transfer To cite this version : HAL Id : lirmm-00108801," 2006.
15. Kumar, B. S., Raj, V. R., & Nair, A. (2017, April). Comparative study on aes and rsa algorithm for medical images. In 2017 International Conference on Communication and Signal Processing (ICCSP) (pp. 0501-0504). IEEE.

AUTHORS PROFILE

ThejasBharathan ,MCA(Masters of Computre Application) , Amrita School of Arts & Sciences, Amrita Vishwavidyapeetham, Mysore, karnataka, India.

Santhosh Kumar B J, Asst. Professor , Department of Computer Sciences , Amrita School of Arts & Sciences, Amrita Vishwavidyapeetham, Mysore, karnataka, India