International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 07 | July 2021 www.irjet.net p-ISSN: 2395-0072

Framework on Secure File Repository in Cloud using Hybrid Cryptography Techniques

Akash Phad[1], Abhijit Shinde[2], Akshay Lukaday[3], Suraj Chandugade[4], Nikhilkumar Shardoor[5]

[1,2,3,4,5]*Department of Computer Science Engineering, MIT School of Engineering, MIT-ADT University, Pune, Maharashtra, INDIA*

Abstract - In recent years network security has become an important issue. Encryption has come up as a solution and plays an important role in the information security system. Many techniques are needed to protect the shared data. The present work focuses on cryptography to secure the data while transmitting in the network. Firstly the data which is to be transmitted from sender to receiver in the network must be encrypted using the encryption algorithm in cryptography, user selects via which technique he wants to encrypt/decrypt data. Secondly, by using the decryption technique (as per the user's choice), the receiver can view the original data. Key is sent via Email using steganography.

Key words - AES, cryptography, steganography, RSA, DES, decryption

1. INTRODUCTION

The data encryption is the process by which a plaintext is converted into an encrypted form (unreadable) and it can only be accessed by authorized person/parties. Data security is a key component of an individual/organisation; it can be done using several techniques. The encrypted data will be protected for a while but will never be safe. After the time has elapsed, the hacker will hack the data. Fake files are sent in the same way that the encrypted data may be sent. Security of the network prohibits unwanted access to data within a network. It involves the authorisation of access to information across a network. and it is measured by network administrators. The requirement for security is to safeguard information, to ensure that resources are accessed and authenticated and that resources are available.

In recent years, network security has become a major concern. Encryption has been developed as a solution and is an essential part of the security system of information. To safeguard the shared data many strategies are required. This paper concentrates on cryptography to safeguard the data during network transmission. First, data that are to be transferred from a sender to a recipient on the network has to be encrypted by means of cryptographic encryption algorithms, whereby user picks the method of encrypting / decrypting data. Second, the receiver can access the original data with the decryption method (as selected by the user). Key is sent via Email using steganography.

2. LITERATURE SURVEY

AES and RSA were used to create hybrid cryptography in [1]. The symmetric key used for message encryption is also encrypted in this hybrid cryptography, which improves security. This document also includes the ability to construct a digital signature by encrypting the message's hash value. This digital signature is used to confirm the integrity of the message at the other end. The encrypted message, encrypted symmetric key, and encrypted digest are then concatenated to generate the final message. The LSB steganography method was used to encrypt this entire message once more. In this case, hybrid cryptography and steganography improves and strengthens security. This algorithm has a unique feature called message integrity checking. The practicality of this approach has been demonstrated by successful simulations.

Shows [2] implemented a new hybrid cryptosystem. The primary goals of this study are to stress improved performance, maximum speed of an algorithm, effectiveness testing, and comparisons with other algorithms. Two new hybrid algorithms are proposed in the paper, which combine symmetric and asymmetric cryptographic methods like Twofish, AES, RSA, and ElGamal. JAVA programme implementation was utilised to examine results. The results demonstrate that the suggested hybrid algorithm AES+RSA is extremely secure. Other advantages of the Twofish + RSA hybrid include improved computation speed, cypher text size, and memory usage.

It [3] suggested a fledgling picture mapping approach for encoding the message into relative concentration by scrambling plain content information into HEXADECIMAL. The different Hex properties are put together to make a framework. PRNG (Pseudo Random Number Generator) circuits are the foundation of cryptographic structures.This [4] compares the security and PSNR (peak signal-to-noise ratio) of conventional RDH (Reversible Data Hiding) and LSB (with encryption) algorithms with enhanced RDH algorithm.

It [5] presented a three-layered architecture for protecting message sharing mechanisms, with the QR code picture as one of the layers. This design makes use of cryptography and steganography techniques in a purposeful and empirical way. On the basis of quantitative and qualitative data, the suggested system provides a higher level of security.Furthermore, the system was

accessed using the performance evaluation criteria outlined in the study.

Using traditional encryption techniques to provide security has become more difficult in recent years. Combining two standard encryption techniques is recommended to avoid this vulnerability.One scenario is that the attacker is unaware of the ciphertext and enciphered key. The likelihood of an attack is nil. On the other hand, if the hacker has the cipher key, he can obtain the plaintext image using the private key.When compared to other current methods, the technique suggested in [6] is more resilient and provides superior security. MATLAB is used to implement it.

The existing encryption approaches, such as AES, DES, and RSA algorithms, as well as the LSB replacement technique, were examined in a study [7]. Those encryption approaches have been thoroughly researched and examined in order to improve the performance of the encryption methods while also ensuring security. Based on the results of the experiments, it was determined that the AES method uses the least amount of encryption and decryption time, as well as the least amount of buffer space, when compared to the DES algorithm. RSA, on the other hand, takes longer to encrypt data and uses a lot of memory. We also found that the AES algorithm's decryption is superior to those of other algorithms.

The research paper [8] is focused in securing transmission of Meteosat pictures on the Internet, in public or local networks. A hybrid encryption algorithm based on the Advanced Encryption Standard (AES) and the Rivest Shamir Adleman (RSA) algorithms is proposed to improve the security of the Meteosat transmission in network communication. Due to its higher block encryption and management benefits in key cypher AES is used for data transmission with the AES algorithm and RSA is used for encryption of the AES key. Each new encryption session is created by our encryption system with a unique password.

In the research paper[10], the various performance factors such as key value, computational speed and adjustability are discussed. They concluded that the better AES algorithm between the Symmetric and the better solution with the asymmetric encryption techniques is the RSA algorithm.

Different experimental factors will be analysed in the research paper[11]. Due to the use of text files and experimental results, the time of encryption of the DES algorithm and the use less of the AES algorithm was established in AES algorithms and DES algorithms. RSA also consumes more time of encryption and memory usage is very high, but RSA algorithm uses output byte at least.

In research paper[12], all techniques were found to be useful for encryption in real-time. Each technology is unique and can be adapted for various applications. New encryption techniques are evolving every day, and conventional encryption technology is therefore developing quickly and safely, with great security.

A new comparative study among encryption technology was presented in the research study[13], which includes nine factors: the main length, the cypher type, the size of the block, its development, its crypt-analyses resistance, security, the possible option key and ACSII printable type key keys.

DES is a secret, key-based algorithm that suffers from key distribution problems and key agreement issues. In the research paper[14] However, RSA takes a great deal of time to do encryption and decryption. It has also been observed that decrypting DES algorithms is better in performance and lower energy consumption than other algorithms.

3. PROPOSED SYSTEM

Figure 3 illustrates a proposed security system that uses cryptographic and steganography techniques.The Django framework is used to create a website that allows users to register. After registering, the user logs in to the portal using their user ID and password. The user has the option of using any of the two algorithms from AES, DES and RSA to encrypt the files which they previously uploaded. The encrypted file is then stored in cloud(firebase server), from server receiver collects and decrypt the file.To decode the file, the user will need a key, which will be e-mailed to the authorised person. Keys are encoded using steganography. The secret messages in steganography can be hidden in various multimedia files such as text, sound, photos, animations, video, and so on; in this system, we will hide our key inside an image.

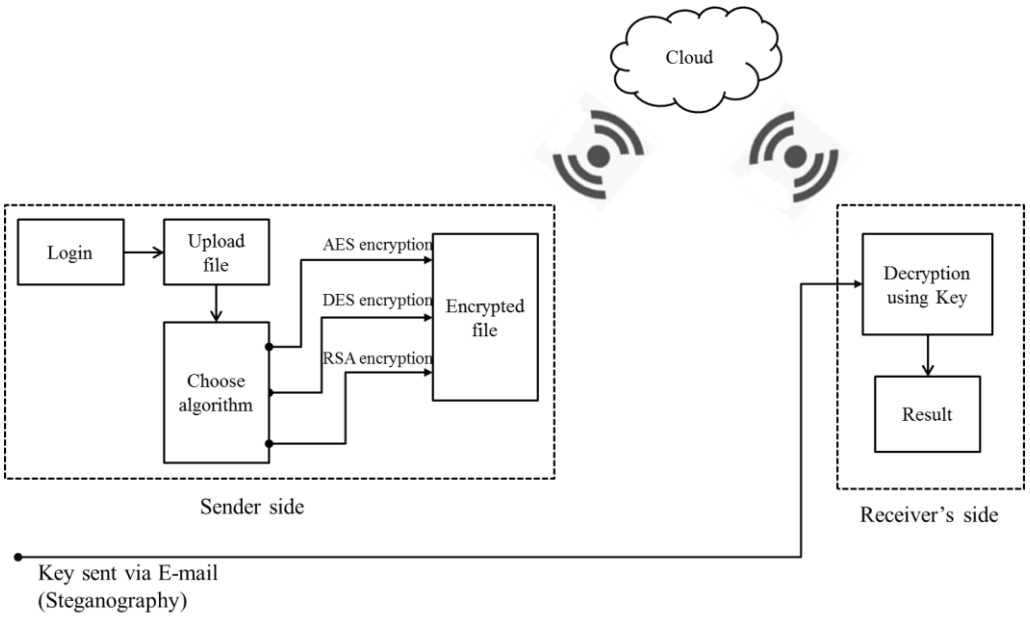

Figure. 1 Proposed System

4. MATHEMATICAL MODEL

Mathematical model of proposed system can be described using set theory. Let M be a set containing all algorithms

$$M = \{A, B, C\}$$

Here A is AES algorithm

B is DES algorithm and

C is RSA algorithm

For encryption user will choose combination of any two algorithm out of three. The combination of selected encryption algorithm is represented by EA and it is given as

$$EA = \ any\ two\ \{A, B, C\}$$

Information provided by user is divided into two equal parts, data1 and data2.

$$data = \{data1, data2\}$$

As data is encrypted by using combination of two algorithms, two different keys S1 and S2 are required, where S1is key for 1st algorithm whereas s2 is for 2nd selected algorithm.

$$S1 = \ key\ [EA1]$$

$$S2 = \ key\ [EA2]$$

To encrypt a data we need combination of selected algorithm, a key and data which has to be encrypted. The encrypted data is represented as:

$$Y = \left\{S1 \bigotimes data1 + s2 \bigotimes data2\right\}$$

Where, data is the information user wants to encode and send. Key S1 and data data1 are convolved and concatenated with S2 and data2.

Information as "Y" is sent to user via cloud. The encrypted data must be decrypted using key "S1" and "S2" which user received via E-mail. S1 and S2 are encrypted using steganography. Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. For steganography we convolved image, S1 and S2. KS is secure key.

$$KS = \ image \bigotimes S1 \bigotimes s2$$

At the receiver side, for recovering key $S1 \otimes S2$, following process is carried out

$$S1 \bigotimes S2 = image \bigotimes KS$$

Decryption process is given as:

$$data' = \ decrypt\ \{Y \otimes S1 \otimes S2\}$$

data' is decrypted information, for secured transferring of information *data'* must be identical to *data*.

Confidentiality of information is checked by comparing original information with decrypted information:

If data=data'

Authenticate file

If data ≠ data' File is Tempered

5. IMPLEMENTATION

Firstly the user need to sign-up into the system after that user can login into the system using login credentials.

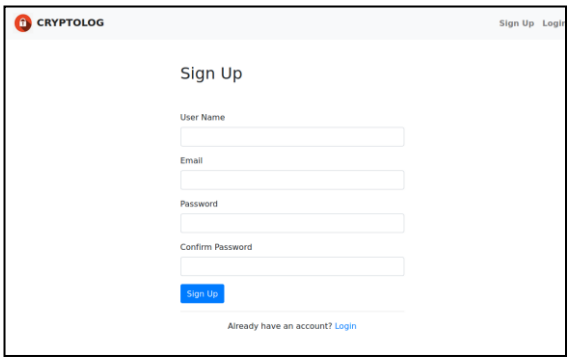

Figure 5. Sign-up Form

If user wants to send the text file to some another user securely, then the sender has option to encrypt the file using combination of cryptography algorithms i.e AES & RSA, DES & RSA and AES & DES.

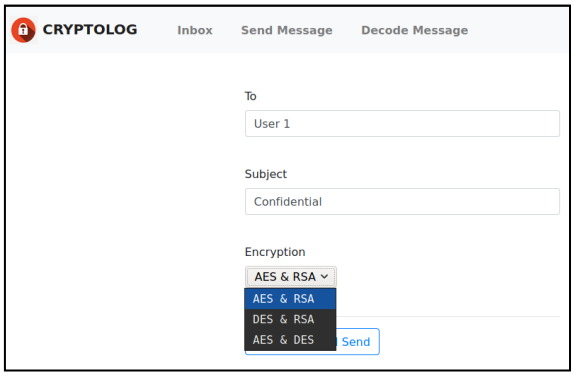

Figure 6. Select Encryption Type

The text file which user wants to send is divided into two equal half and then each half is encrypted using different algorithm. Then whole encrypted file is send to the receiver with a subject name. While sending the encrypted file, we share the key with the receiver via email using steganography. The key is embedded into the image and it is send to receiver's Email ID so that receiver can decrypt the file.

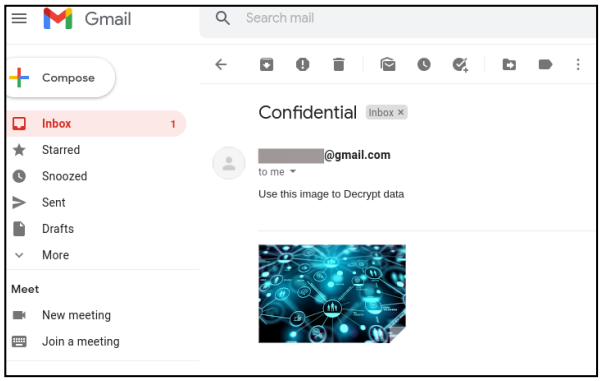

Figure 7. Steganography Image via Email

Encrypted file also gets saved in the firebase as shown below.

Figure 8. Encrypted File in Firebase

Figure 9. Encrypted Information in File

After the receiver receives the encrypted file with some subject name, receiver has option to decode the file and download it.

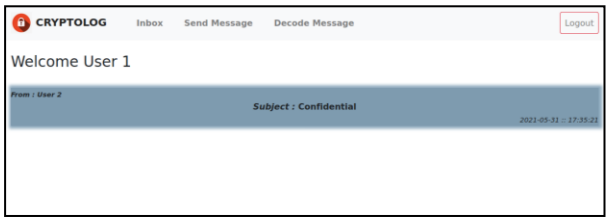

Figure 10. File Received With Subject Name

For decoding the encrypted file user has to provide the subject name and the steganography image. The receiver has to download the steganography image which has key embedded in it and is send by the sender from his/her Email. Then the receiver need to upload the steganography image into the system to successfully decode the encrypted file.

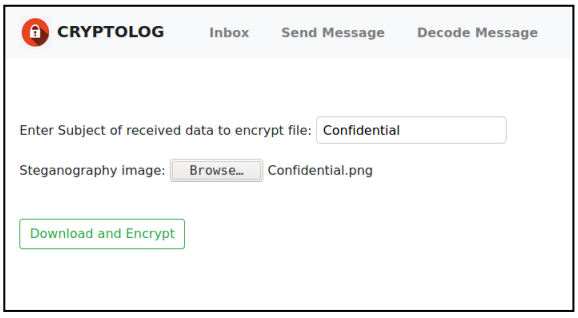

Figure 11. Decoding Process

6. Conclusion

Every cryptographic algorithm has weaknesses and strengths. The encryption algorithm must be selected based on the applications requirements to be implemented. If secrecy and integrity are important considerations, the AES algorithm can be used. If the application's needs is network bandwidth, the DES is the best solution. In this paper, hybrid cryptography and steganography were used, and a stego picture was created. The message is here encoded using AES, DES and RSA (the choice of user). All the encrypted files, i.e. the encoded message, the encrypted key and digest were concatenated to create a full message. We have used cryptographic algorithm like DES, AES and RSA along with the steganography technique for hiding the document in an image file. Our future work will focus on SLSB as the replacement for LSB technology (steganography technique).

References

[1] Biswas, Chitra; Gupta, Udayan Das; Haque, Md. Mokammel (2019). [IEEE 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE) - Cox'sBazar, Bangladesh (2019.2.7-2019.2.9)] 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE) - An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography. , (), 1–5. doi:10.1109/ECACE.2019.8679136

[2] Jintcharadze, Elza; Iavich, Maksim (2020). [IEEE 2020 IEEE East-West Design & Test Symposium (EWDTS) - Varna, Bulgaria (2020.9.4-2020.9.7)] 2020 IEEE East-West Design & Test Symposium (EWDTS) - Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems. , (), 1–5. doi:10.1109/ewdts50664.2020.9224901

[3] Patel, Urvi; Dadhania, Pradish (2019). [IEEE 2019 Innovations in Power and Advanced Computing Technologies (i-PACT) - Vellore, India (2019.3.22-2019.3.23)] 2019 Innovations in Power and Advanced Computing Technologies (i-PACT) - Multilevel Data Encryption Using AES and RSA For Image and Textual information Data. , (), 1–5. doi:10.1109/i-PACT44901.2019.8960227

[4] Rashmi, N.; Jyothi, K. (2018). [IEEE 2018 2nd International Conference on Inventive Systems and Control (ICISC) - Coimbatore, India (2018.1.19-2018.1.20)] 2018 2nd International Conference on Inventive Systems and Control (ICISC) - An improved method for reversible data hiding steganography combined with cryptography. , (), 81–84. doi:10.1109/ICISC.2018.8398946

[5] Mendhe, Abhijeet; Gupta, Deepak Kumar; Sharma, Krishna Pal (2018). [IEEE 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC) - Jalandhar, India (2018.12.15-2018.12.17)] 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC) - Secure QR-Code Based Message Sharing System Using Cryptography and Steganography. , (), 188–191. doi:10.1109/ICSCCC.2018.8703311

[6] Mahalakshmi, B.; Deshmukh, Ganesh; Murthy, V.N.L.N (2019). [IEEE 2019 Fifth International Conference on Image Information Processing (ICIIP) - Shimla, India (2019.11.15-2019.11.17)] 2019 Fifth International Conference on Image Information Processing (ICIIP) - Image Encryption Method Using Differential Expansion Technique, AES and RSA Algorithm. , (), 363–366. doi:10.1109/ICIIP47207.2019.8985665

[7] B. Padmavathi1 , S. Ranjitha Kumari, "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064 Volume 2 Issue 4, April 2013

[8] 1Boukhatem Mohammed Tizi-Ouzou, Cherifi Mehdi, "Meteosat Images Encryption based on AES and RSA Algorithms Meteosat Image Encryption", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 6, 2015

[9] Dr. Prerna Mahajan & Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013 Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc. (USA) Online ISSN: 0975-4172 & Print ISSN: 0975-4350

[10] [1] AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram "Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.3033-3037

[11] Shashi Mehrotra Seth, Rajan Mishra "Comparative Analysis Of Encryption Algorithms For Data Communication" IJCST Vol. 2, Issue 2, June 2011 I S N : 2 9 - 4 3 (P r i n t) | I S S N : 0 9 7 6 - 8 4 9 1 (On l i n e)www. i j c s t. c o m

[12] E.Thamiraja ,G.Ramesh,R.Uma rani "A Survey on Various Most Common Encryption Techniques"

International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012 ISSN: 2277 128X

[13] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani "New Comparative Study Between DES, 3DES and AES within Nine Factors" Journal Of Computing, Volume 2, Issue 3, March2010,Issn2151-9617

[14] Aman Kumar , Dr. Sudesh Jakhar , Mr. Sunil Makkar "comparative analysis between DES and RSA algorithm" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012 ISSN: 2277 128X.

[15] Akash Phad, Akshay Lukaday, Abhijit Shinde, SurajChadugade, Nikhilkumar B Shardoor "Protected File Repository in Cloud Using Crossbreed Cryptography" IRJET Volume: 08 Issue: 02 | Feb 2021| e-ISSN: 2395-0056 p-ISSN: 2395-0072.

BIOGRAPHIES

Akash Phad This author is pursuing Bachelor degree in Computer Science and Engineering in MIT School of Engineering, MIT ADT University, Pune, Maharashtra, India. He has specialization in the field of Network Security. He has also interest in the field of wireless sensor network.

Nikhilkumar B Shardoor Assistant Professor in MIT ADT UNIVERSIY, Pune. Research Scholar, PhD (Regd.) in Computer Science Engineering, GITAM University, Vizag. Area of Interest Data Analytics, Machine Learning, Cloud Computing and IOT.

Akshay Lukaday This author is pursuing his Bachelor degree in Computer Science Engineering, in MIT School of Engineering, MIT ADT University, Pune with Network and Security as a specialisation. As security domain is concerned, he has done Cybersecurity specialization from Amazon web Services and Cyber security Essential from Cisco.

Abhijit Shinde This author is currently pursuing his Computer Science degree from MIT ADT University Pune, Maharashtra. He has a keen interest in Cybersecurity field.

Suraj Chandugade This author is a B. Tech student of Computer Science and Engineering, at MIT School of Engineering, MIT ADT University, Pune. With the Network and Security as the specialisation. His research is concerned with Secure data communication in the field of message broadcasting Networks. As regards the Security Domain, Cyber Security Specialization from Amazon Web Services and Cybersecurity Essential from CISCO has been completed. He has interest in the field of Network Security, Software development (DevOps and Web development.