International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Establishing a Secure File Transfer Using Hybrid Cryptography and LSB Stenographic Techniques

K Annsheela[1], S Habeeb Mohamed Sathak Amina[2]

[1 2]Assistant Professors, Department of Computer Science and Research Centre, Thassim Beevi Abdul Kader College for Women, Kilakarai.

Abstract: ***The transfer of files or data in a secure manner is prevalent. Security is the primary concern while transferring files or data. It is highly beneficial to use cryptographic techniques to secure data. They can transferable between the nodes. Steganography and cryptography are being used more to protect data. Using a single algorithm to transfer data with high security levels is ineffective. Give a novel approach to security in this work by applying steganography and the symmetric key cryptographic algorithm. Data is protected by the proposed system using block - wise security algorithms AES, which stands Advanced Encryption Standard is an algorithm that uses the same key to encrypt and decrypt protected data. DES, which stands Data Encryption standard is an uses symmetric keys, which means that the same key is used for encrypting and decrypting the data and the RC2 is a variable - key - size block cipher. LSB steganography technique is introduced for key information security***

Keywords: Networking, AES algorithms, DES algorithms, RC2 new security mechanism using symmetric key cryptography algorithm and steganography, LSB algorithms

1. Introduction

Networking is utilized to send massive amounts of data in a variety of settings, including industry, military colleges, etc. The can be moved among the nodes. There are numerous problems with the data transfer. The original data is transformed via cryptography into an unreadable format. Symmetric key cryptography and public key cryptography are two types of cryptography. This method use keys to convert data into unintelligible form in order to address these problems in a variety of ways. The use of steganography and cryptography for data protection is growing in popularity nowadays. It is ineffective to transport data with high levels of security using a single algorithm. In this research, symmetric key cryptography technique and steganography are used to introduce novel security mechanism.

2. Objectives

This system's primary goal is to safely store and retrieve data that is only accessible by the data owner on the cloud. Cryptography and steganography techniques are used to overcome data security challenges related to cloud storage. The DES, RC2, and AES algorithms are used to secure data. Cloud storage systems are secured using the hybrid cryptography paradigm, which uses AES for text or data encryption and RSA for key encryption. Block cypher RC2 has a changeable key size. For important information security, the LSB steganography technique is presented.

3. Literature Survey

A literature review is nothing but an objective, aim, or summary of whatever research has done relevant to a certain topic. The following published articles have been referred to create a base for my project. Following are some papers been referred to: -

1) M. Malarvizhi, et. al [3] mentioned this paper is on the integrity of files and restoring the files if integrity is violated. The proposed system uses a pattern of each protected file to determine its modification. The method used for pattern generation is cryptographic hash functions. The system also uses a database that stores the files that need to be protected and their hash codes. To check the integrity of the file the hash code of the file is produced and checked with one in the database. If the file is successfully tested positively then access is granted otherwise the administrator gets alerted and if it is saved copy is available of the same file, then the file is restored
2) Jerzy Kaczmarek, et. al [3], described this paper describes an approach to the integrity of files and restoring the files if any problem is arising in the future. This proposed course uses a pattern of each protected file to determine its modification. Methods used for pattern generation are cryptographic hash functions. This system uses a database that stores the names of all files.
3) V. S. Mahalle, et. al [2] applied hybrid cryptography technique for securing data on cloud storage. A hybrid encryption and decryption algorithm using RSA and AES algorithms was proposed. The paper was only focusing on administrative unaware uploading and downloading of data by maintaining its integrity. Further the key distribution was very secure because three keys are distributed for doing encryption and decryption. A unique key generation technique was used to make the process more secure.
4) Aditya SadanandGhadi [1] mentioned the paper some symmetric key cryptography techniques in addition to stenography techniques. The idea of splitting and merging adds on to meet the principle of data security. This hybrid approach when implemented in a cloud server makes the remote server more secure and thus, helps the cloud providers to do their work more securely. For data security and privacy protection problems, the fundamental challenge of separation of sensitive data and access control is fulfilled.

4. Implementation and Methodology Used

In this paper, LSB Steganography technique algorithm are used. Create a various models and analysis are made. Then data or file are transferred using Hybrid Cryptography.

Models:

- Node Details
- User Interface Design
- Data Transfer
- Encryption Phase
- Decryption Phase

Node Creation:

Nodes are the building blocks of the Network. They can play multiple roles in the network. Such as data processing, data storage and routing. The nodes can be created or deleted by the administrator firmly. The details like IP address, size and position of the nodes will be maintained in the database.

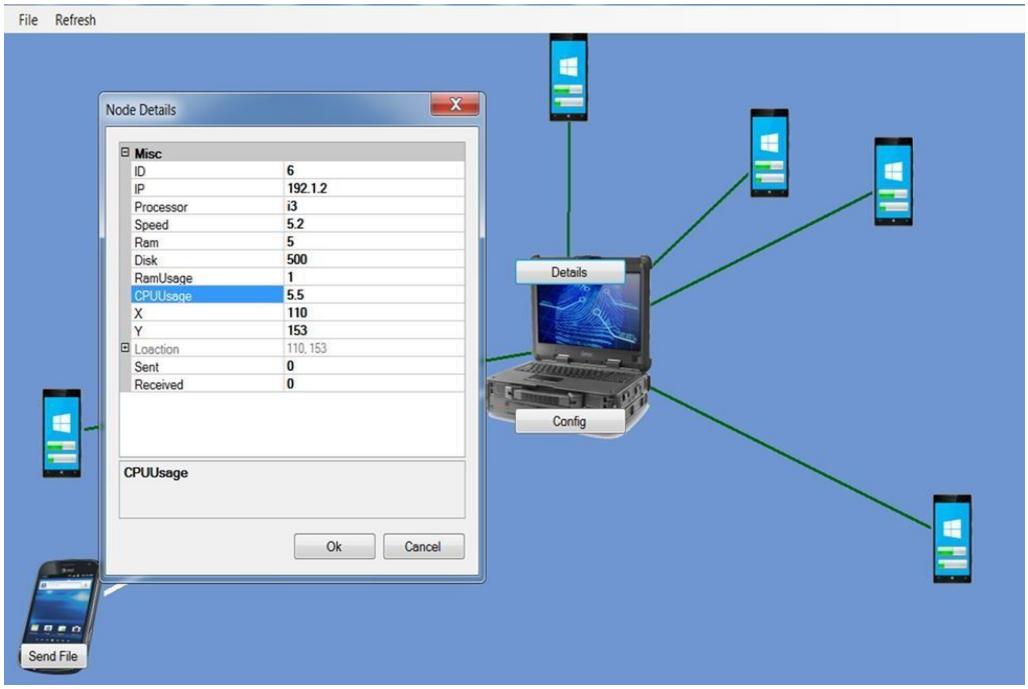

Figure 4.1: Node Creation

User Interface Design

It provides the way for users to interact with the system information and it mainly meant for security issues. In this project, this is the main module i. e. front sheet where user needs to register them by given the name, mobile number, username and password. The encrypted token will be generated for each user. The user enters into the system with username and password. This will show the decent security of this project.

Figure 4.2: User Interface Page Creation

Data Transfer:

This module is responsible for transferring the data in the network. The data can be transferred from one node to another node in encrypted form. These transferring times, file size and file name will be maintained in the database. The data can be decrypted by giving the decryption Keys.

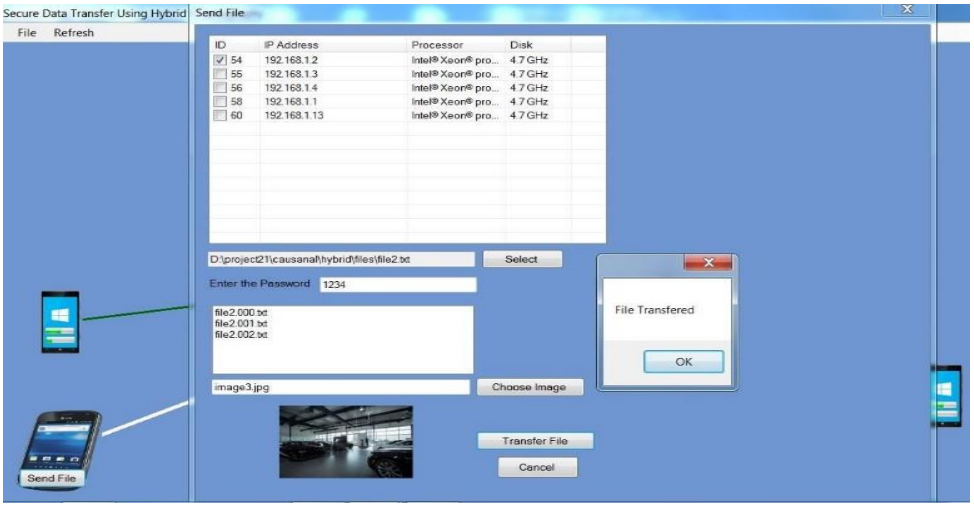

Figure 4.3: Data transfer using encryption and decryption

Encryption Phase

Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret Key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text. At the encryption end, the file being spitted into three blocks and each block will be encrypted AES, DES and RC2 algorithms. The encrypted keys will be compressed into the image.

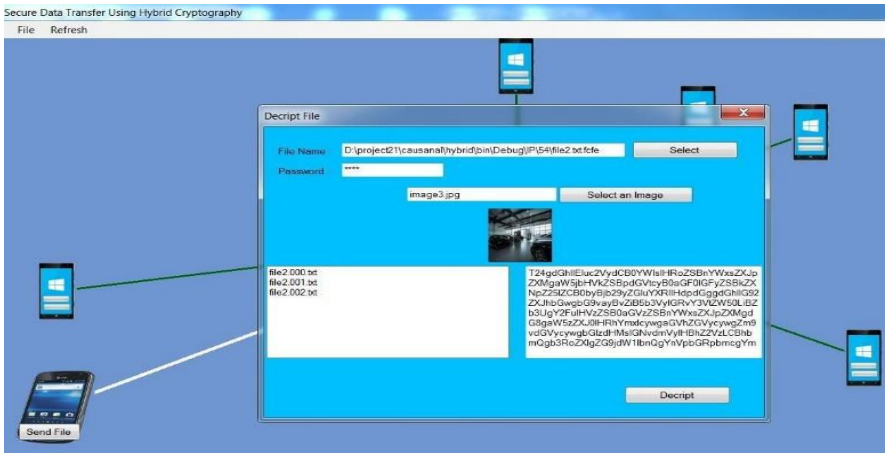

Figure 4.4: Encryption used by AES, DES, and RC2 Algorithms

Decryption Phase

The key image will be sent to the end user's email. This will be downloaded and entered by the valid user to get the decryption keys. The LSB technique will be implemented to extract the decryption keys from the image. The combination of decryption keys will provide the original data.

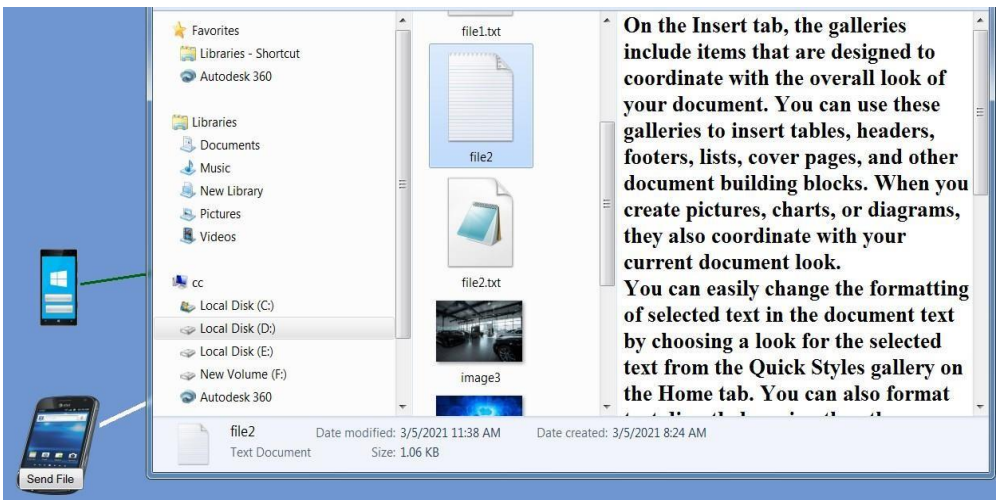

Figure 4.5: Decryption used by LSB Technique

5. Results

Data stored in files can be accessed or retrieved on the users request without direct access to the server computer. This Security problem can be solved using several different ways, cryptography and steganography are the most commonly used techniques. But sometimes a single algorithm alone cannot provide security that is required.

6. Conclusion and Future Work

The main objective of this system is to securely transfer data among data receivers and senders across networks. Techniques from steganography and cryptography are used to resolve network data problems. Using the RC2, DES, and AES algorithms, data security is accomplished. Key data is securely preserved with the use of LSB technology (Steganography). Using the multithreading technology, the encryption and decryption procedure takes less time. The suggested security technique has allowed us to achieve improved data integrity, high security, low latency, authentication, and confidentiality. In the future, public key cryptography can be introduced to prevent assaults during data transmission through the network, and it can be used promptly.

References

[1] V. S. Mahalle and A. K. Shahade, "Enhancing the data security in Cloud by implementing hybrid (Rsa&Aes) encryption algorithm, " 2014 International Conference on Power, Automation and Communication (INPAC), Amravati, 2014, pp.146 - 149. doi: 10.1109/INPAC.2014.6981152

[2] A. A. Kumar, Santhosha and A. Jagan, "Two layer security for data storage in cloud, " 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), Noida, 2015, pp.471 - 474. doi: 10.1109/ABLAZE.2015.7155041

[3] Singh, G., Supriya, A study of encryption algorithms (RSA, DES, 3DES and AES) for information security, International Journal on Computer Applications, 2013; Volume 67, Issue 19.

[4] Rani, S. and Kaur, H., Implementation and comparison of hybrid encryption model for secure network using AES and Elgamal. International Journal, 2017; 8 (3).

[5] Harini, M., Gowri, K. P., Pavithra, C. and Selvarani, M. P., A novel security mechanism using hybrid cryptography algorithms. Electrical, Instrumentation and Communication Engineering (ICEICE), IEEE, 2017.

[6] L. M. Kaufman Data security in the world of cloud computing IEEE Security & Privacy (2009)

[7] B. Swathi, 2 Sri. Dr. Bhaludra Raveendranadh Singh, "Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm, "Volume no.06, Issue No.11, November 2017.

[8] Tingyuan Nye and Tang Zhang "An investigation of DES and Blowfish encryption algorithm", in Proc. IEEE Region 10 Conference, pp.1 - 4, Jan.2009. [11]Peter Mel and Tim Grace, "The NIST Definition of Cloud Computing", NIST, 2010.

[9] Gupta, N., Kapoor, V.: Hybrid cryptographic technique to secure data in web application. J. Discret. Math. Sci. Cryptogr.23, 125–135 (2020)

[10] Introduction to cryptography and types of cryptography, RobMardisalu. https: //thebestvpn. com/cryptography/

[11] Rewagad, P., & Pawar, Y. (2013). Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing.2013 International Conference on Communication Systems and Network Technologies.

[12] Fortine Mata, Michael Kimwele, George Okeyo, "Enhanced Secure Data Storage in Cloud Computing Using Hybrid Cryptographic Techniques (AES and Blowfish) "

[13] Shaikh, S., & Vora, D. (2016). Secure cloud auditing over encrypted data.2016 International Conference on Communication and Electronics Systems (ICCES). doi: 10.1109/cesys.2016.7889842

[14] Kranthi Kumar K, Devi T, (2018). Secured Data Transmission in Cloud Using Hybrid Cryptography. International Journal of Pure and Applied Mathematics, 119 (16), 3257 - 3262

[15] https: //www.researchgate. net/publication/339722778_Hybrid_cryptography_and _steganography_method_to_embed_encrypted_text_m essage_within_image#: ~: text=Rahim%2C, Physics%3A%20Conference%20Series

[16] Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm", Punam V Maitri and Aruna Verma (2016), IEEE

[17] O. Hosam and M. H. Ahmad, "Hybrid design for cloud data security using combination of AES, ECC and LSB steganography, " Int. J. Comput. Sci. Eng., vol.19, no.2, pp.153–161, 2019.