WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cloud Based Secure File Storage using Hybrid Cryptography

Srinidhi Kulkarni[1], Manjesh M[2], Nithish R[3], Sharanya R P[4]

[1]Department of Computer Science and Engineering Jyothy Institute of Technology Bengaluru, India srinidhi.kulkarni@jyothyit.ac.in
[2]Department of Computer Science and Engineering Jyothy Institute of Technology Bengaluru, India manj9sh@gmail.com
[3]Department of Computer Science and Engineering Jyothy Institute of Technology Bengaluru, India nithishraju24@gmail.com
[4]Department of Computer Science and Engineering Jyothy Institute of Technology Bengaluru, India sharanyarp2502@gmail.com

ABSTRACT—

This survey proposes a method to urge secure encryption and decryption of data utilising a mix of both cryptography and steganography, combining hashing, encryption, and information concealing to increase the privacy of file storage. Recent innovations to employ steganography to encrypt private communications, digital images, or other information have made stego analysis increasingly challenging. By using stego analysis, it is possible to swiftly determine whether carrier files contain any hidden information. A brand-new steganographic technique for private communication between two people is presented in this project. This project's methodology combines steganographic and cryptographic techniques. RSA is a cryptographic algorithm. We utilise picture steganography to conceal data in steganography. In order to offer Access Control, Confidentiality, Integrity, and Authentication for all cryptographic services, we also use the Mutual Authentication technique. In this approach, we can preserve the data more securely. Since we utilise the RSA technique to encrypt the data, we can use Steganography to cover it up in an image, preventing unauthorised network users from accessing the data that is now being stored. The message or the data cannot be retrieved by anybody other than the recipient and its initiator.

Keywords— cryptography, hybrid cryptography, cloud storage, file storage, AES, DES, RSA, LSB.

I. INTRODUCTION

Numerous Internet apps that use digital communication experience noteworthy and ongoing growth. As a result, secure communication sessions must be made available. Data security during transmission over a worldwide network has become crucial to gauging the effectiveness of the network. As a result, data confidentiality and integrity are necessary to stop eavesdroppers from accessing and utilizing transmitted data. Network security is provided by a variety of approaches including steganography and cryptography. This aim of this survey is to provide a novel method of concealing sensitive information in images by combining steganography with encryption.

The term "cloud" really refers to the process of storing data in an external storage system that is managed by a different party. You store data somewhere else rather than retaining it on your computer's hard disc or another local storage device.

Cryptography provides significant benefits for information security. Information security is significantly impacted by cryptography. It is a method for keeping data in a specified format and transferring it so that only the intended audience may access it.. Greek words kryptos (krnptos), indicating sneaky or secret, and praphia (graphia), simply means to write, were used to create the word "cryptograph".

Cryptographic algorithms: Here, methods for guaranteeing information's confidentiality and/or validity are studied.

A. Symmetric Cryptography

A secret key and an encryption algorithm are used in symmetric encryption to convert plaintext into cipher-text. The cipher-text is decrypted with the same key using an algorithm to restore the plaintext.

B. Asymmetric Cryptography

Different keys are used to encrypt and decode data in asymmetric key encryption or public key cryptography. In this approach, each communication's participant has two keys: a public key that is known by all participants and is kept secret, and a private key that is only known to the intended recipient. Despite appearing to be distinct, the public and private keys are mathematically connected. There is a matching private key for each public key. This method can offer nonrepudiation, integrity, and authenticity

C. Steganography

It might be defined as the science of disguising the transmission of data across allegedly reliable channels. As a result, the existence of the message was unknown beforehand. The person would not attempt to decode it if they were to look at the cover that the content was sealed inside since they could not

be aware that there was any covering data inside.The cover media may contain secret information that was introduced by the stego system encoder using a particular algorithm..

D. Various forms of steganography:

a. Text Files

Text stego is the term used to describe the practise of hiding information inside text. Due to the fact that this sort of file can only hold text files, text steganography requires less Memory. It allows for quick file transmission or transfer between sender and recipient.

b.Image Files

It is the process through which we incorporate data into picture pixels. in order to prevent the attackers from seeing any changes to the cover picture. A popular picture steganography algorithm is always LSB method.

c. Audio Files

It is the method through which we conceal information within an audio file. There are several methods for concealing sensitive information in audio recordings for examples Phase Coding, Least Significant Bit (LSB).

d. Video Files

The idea behind it is to hide certain private information among video frames.

II. LITERATURE SURVEY

Paper Title	**Algorithm Used**	**Strength**	**Weaknesses**	**Author(Date)**
"Triple Security of Data in Cloud Computing"	DSA, AES and Steganography	The Digital Signature Algorithm (DSA), the Advanced Encryption Standard (AES), and step-by-step steganography methods were proposed as a mechanism for cloud security. It is first encrypted using DSA for authentication, then for encryption AES is used, for extreme security, Using steganography,content is masked within an audio file.	Due to the one-by-one nature of the research, temporal complexity is substantial..	Garima and Naveen (2014)
"Secure Cloud Auditing over Encrypted Data"	ElGaman and SHA-256	Boost the method for data integrity checking that is outsourced. By using cryptography techniques, the implicit cloud security issue is resolved. In three instances, implicit cloud security is offered.	RSA's encryption and decryption processes take longer.	Deepali and Sarah (2016)
"Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm"	Blowfish, AES&RC6	Data security is handled on a block-by-block basis.	Data encoding and decoding are performed with minimum downtime and low privacy using DES, Blowfish and AES.	Aruna Verma and Punam V Maitri (2016)

"A Novel Security Mechanism Using Hybrid Cryptography Algorithms"	AES and RSA	to lessen data transmission costs, optimize data transfer rate, and tighten privacy.	Hash values are also no more considered in secure cryptography	Bhale (2016)
"Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm"	BRA, blowfish, RC6 algorithm	The suggested security method aids in meeting the information integrity, highly secure, reduced latency, validation, and secrecy criteria.	Utilise hybridization of public key cryptography methods to achieve high levels of security can be improved	Punam V. Maitri (2016)
"HybridAlgorithmforCloudDataSecurity"	MD5andAES	Tackle four phases(RegistrationofCloudUsertoCloudServiceProvider),Storing of Datain CloudStorage,UserAuthenticationon DataRetrievalRequestand retrival of data and integrity verification	utilises a single hashing method and cryptographic technique. Additionally, MD5 hashes are no longer thought to be very secure for cryptography.	RichaS andRichaD. (2017)
"Securefilestorageinclo udcomputingusinghybri dcryptography Algorithm"	BlowfishandSRNN publickey	In SPI benefit conveyance models, challenges with information security and protection arise at all levels.	SRNN improves timing performance	B.SwathiandBhaludr a(2017)
"A Hybrid Cryptography Algorithm for Cloud Computing Security"	RSA and SHA2	The suggested approach safeguards user data against unwanted access both during transmission and while it is stored in Storage Service Bucket.	The encryption and decryption procedures for RSA require more time.	Divya Prathana Timothy (2017)
"Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques"	RSAand Diffie-Hellman	While maintaining the authenticity of the reconstructed image, it reduces the most bits.	Huffman coding scans the data twice.	Osama Fouad Abdel Wahab (2021)
"Hybrid Cryptography Algorithm For Secure andLow Cost Communication"	RSA and Diffie-Hellman	In this scenario, two distinctly separate programs collaborate to reliably encrypt and send the information.	The secret key encryption algorithm's key length is larger and requires a lot of bandwidth to broadcast.	Suman Kalyan Ghosh (2020)

"Cloud Security using Hybrid Cryptography Algorithms "	RSA and DES	This security paradigm provides the cloud visitor and service provider with transparency, lowers privacy issues, and accelerates file transmission.	Although different file formats might be examined, just the script has been utilised in this method encryption and decryption..	Sanjeev Kumar (2021)
"ProposedhybridRSA algorithmforcloudcomputing"	RSAANDHMAC	Proposed a framework to address security challenges with cloud computing's authentication and storage levels.		RohiniandErTejinder Sharma(2018)
"Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques"	RSA and Huffman coding	While maintaining the authenticity of the reconstructed image, it reduces the most bits	Huffman coding scans the data twice	Osama Fouad Abdel Wahab (2021)
"Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography"	AES, RSA, SHA and LZW	It permits utilising less cloud storage and offers data transmission safety.		Mustafa S. Abbas (2020)
"Hybrid Cryptography Algorithm For Secure andLow Cost Communication"	RSA and Diffie-Hellman	In this instance, two completely unique programs collaborate to reliably encrypt and transmit the message.	The secret key cryptography algorithm's key size is greater and requires a lot of bandwidth to broadcast.	Suman Kalyan Ghosh (2020)
"Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques"	RSA and Huffman coding	While maintaining the authenticity of the reconstructed image, it reduces the most bits.	Huffman coding scans the data twice.	Osama Fouad Abdel Wahab (2021)
"Cloud Security using Hybrid Cryptography Algorithms "	RSA and DES	This privacy paradigm provides the web user and service provider with transparency, lowers security risks, and speeds up file exchange.	Although different file formats might be examined, only the text file has been utilised in this method' encryption and decryption.	Sanjeev Kumar (2021)

From the above literature survey conducted we can understand from various papers that for any proposed system there will be strength as well as weaknesses involved.

From the above survey we can see that the most common used algorithms to enable highest security using cryptography are AES, RSA, DES, RC6 AND BLOWFISH. We can see that proposing a model only using cryptography might create security breaches.

So to enhance the working of our model with highest security, combination of cryptography with steganography proves efficient along with hybrid algorithms.

From various authors we have understood key management using a stego-image proves to be efficient.

III. OBJECTIVES

This study's primary objectives are:

1) Enabling proper study to understand the various algorithms to ensure highest security.

2) To design a dedicated network model to send and recieve files.

3) To ensure file has highest security using the combination of cryptography and steganography and using algorithms.

4) To create a learning model which enables users without technical knowledge also to use our networking model without any difficulty.

5) To create a dedicated cloud server so the entire amount of data will be only present in our network. This does not allow loss or transmission of used data through eavesdropping

IV. PROPOSED SYSTEM

In this section, we'll talk about a strategy that combines steganography and cryptography, two separate types of techniques used to encrypt data. The message is initially encrypted in this suggested approach using the RSA technique. The encrypted material is then embedded in the visual using the modified LSB approach.. As a result, this technique delivers an extreme level of privacy and combines the advantages of steganography with cryptography. It is better than either approach used by itself. The receiver and the initiator will agree on the keys for the encryption and secrecy algorithms, and these values may be transferred through a private channel of communication. In our approach, data is generally encrypted, later hidden:

Our input is first converted to Base-64 before being encrypted and hidden. The text is subsequently placed inside a text document for storage. The next topics are cryptography and steganography.

Encryption: A hybrid encryption method will be used to encrypt the upload of confidential data to the cloud.

Sender Side:

Steganography and cryptographic phases make up the Sender side. Steganography comes next in this process after cryptography.

Phase of cryptography: We employ the RSA (Rivest, Shamir, and Adelson) algorithm for encryption. Two integers which are prime are essential for that method. The "e" values generated by the two primes can be utilised for encryption as well as Plain Text. The text will then be forwarded to the extreme side to be deciphered and returned to us. This encrypted data will be utilized during the steganographic procedure.

Two Prime integers + Data=Input

Encrypted Data = Output

Stage of steganography:

To conceal data (encoded content from the cryptographic stage) behind a cover, we employ the Least Significant Bit(LSB) technique with minor changes. Although we are using a picture as a cover in our experiment to show how our method works, video and audio files may also use this technique. the standard LSB technique for securing confidential data in a file; , the final bit is utilised sequentially to conceal a single binary stream bits in each pixels, sample, or frame. The cover picture has been encrypted.

Secret key+ cover image+ Encrypted Message = Input

Stego-Image= Output

Receiver’s side:

The stages for both cryptography and steganography are on the receiver's side. We will take the embedded data from the receiving end and then decode it. Steganography Stage

We start with steganography on the receiver side and then switch to cryptography. The identical protocols used by the sender side will be followed by us.

Stego-Image+ Secret Key= Input

Encrypted Message= Output

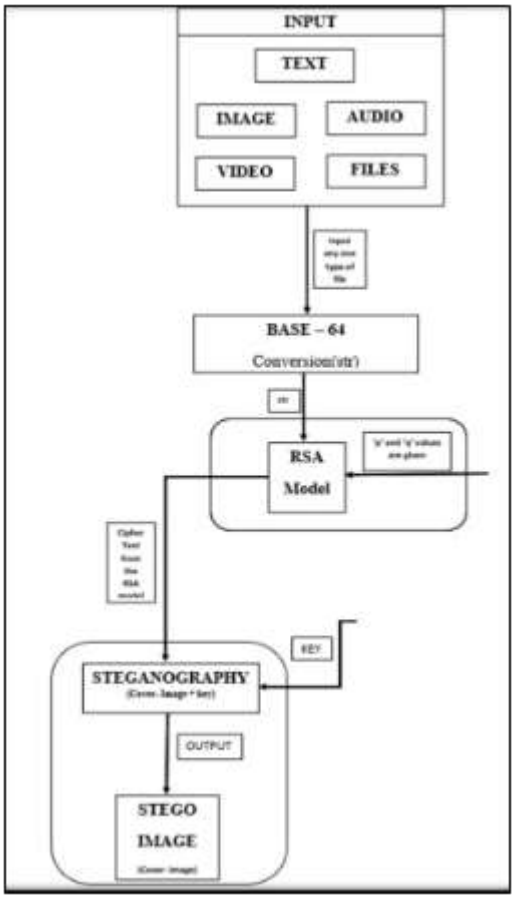
Step of Cryptography:

We'll adhere to the same guidelines as the sender. Decryption can be carried out using the secure communications, the initiator's private key, as well as initiator's public key.

2 Prime Numbers+ Encrypted Message = Input

Plain Text= Output

Plain Text has been replaced by the Base-64 format. To convert the received plain text into the desired input, which may be either Text, Image, Video, or Audio, use Base64 conversion.



V. CONCLUSIONS

Both of the security measures This work successfully combined steganography with cryptography to provide dual protection for information stored in a cloud infrastructure. We've developed hybrids encrypting, which blends the symmetric method AES with the asymmetrical scheme RSA, to protect data kept on the cloud server. The outcomes of hidden data are first encrypted, compressed, and then hidden in the picture using the LSB approach. As more content is enclosed in the picture, the distortions on the picture diminishes when matched to the outcomes using the LSB technique, of information masking without compression. This strategy is more efficient and secure for cyber security in a cloud infrastructure.

REFERENCES

[1] Garima and Naveen (2014), "Triple Security of Data in Cloud Computing", IEEE.

[2] J. V. Karthik and B. V. Reddy, "Authentication of secret information in image steganography," International Journal of Computer Science and Network Security(IJCSNS), vol. 14, no. 6. P. 58. 2014.

[3] S. C. Sukumaran and M. Misbahuddin, "DNA Cryptography for Secure Data Storage in Cloud.," IJ Netw. Secur, vol. 20, no. 3, pp. 447–454, 2018.

[4] “Secure Cloud Auditing over Encrypted Data”, Sarah and Depali (2016),IEEE.

[5] “Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm”, Punam V Maitri and Aruna Verma (2016),IEEE.

[6] R. Shanthakumari and S. Malliga, “Dual-layer security of image steganography based on IDEA and LSBG algorithm in the cloud environment,” Sādhanā, vol. 44, no. 5, p. 119, 2019. [7] “A Novel Security Mechanism Using Hybrid Cryptography Algorithms”, Bhale et.al(2016), IEEE.

[8] “Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm”, Punam V. Maitri (2016), IEEE.

[9] “Hybrid Cryptography Algorithm For Secure andLow Cost Communication”, Suman Kalyan Ghosh (2020),IEEE.

[10] “Cloud Security using Hybrid Cryptography Algorithms ”, Sanjeev Kumar (2021),IEEE.

[11] M. O. Rahman, M. K. Hossen, M. G. Morsad, and A. Chandra, “An Approach for Enhancing Security of Cloud Data using Cryptography and Steganography with E-LSB Encoding,” IJCSNS, vol. 18, no. 9, p. 85, 2018.

[12] S. Shanthi, R. J. Kannan, and S. Santhi, “Efficient secure system of data in the cloud using steganography based cryptosystem with FSN,” Mater. Today Proc., vol. 5, no. 1, pp. 1967–1973, 2018.

[13] A. A. Abdullah, Z. A. Abod, and M. S. Abbas, “An Improvement Steganography System Based on Quantum One Time Pad Encryption,” Int. J. Pure Appl. Math., vol. 119, no. 15, pp. 263–280, 2018.

[14] G. S. Mahmood, D. J. Huang, and B. A. Jaleel, “Achieving an Effective, Confidentiality and Integrity of Data in Cloud Computing.,” IJ Netw. Secur., vol. 21, no. 2, pp. 326–332, 2019.

[15] 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