Secure File Storage using Hybrid Cryptography

2021 6th International Conference on Communication and Electronics Systems (ICCES) | 978-1-6654-3587-1/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICCES51350.2021.9489026

Putta Bharathi
Department of Computer Science & Engineering,
Amrita Vishwa Vidyapeetham,
Amritapuri, India.
bharathi.putta23@gmail.com

Gayathri Annam
Department of Computer Science & Engineering,
Amrita Vishwa Vidyapeetham,
Amritapuri, India.
gayathriannam77@gmail.com

Jaya Bindu Kandi
Department of Computer Science & Engineering,
Amrita Vishwa Vidyapeetham,
Amritapuri, India.
jayabindu49@gmail.com

Vamsi Krishna Duggana
Department of Computer Science & Engineering,
Amrita Vishwa Vidyapeetham,
Amritapuri, India.
vamsikrishnaduggana28@gmail.com

Anjali T.
Department of Computer Science & Engineering,
Amrita Vishwa Vidyapeetham,
Amritapuri, India.
anjaliraj87@gmail.com

Abstract - **Security is a major concern in a wide range of applications, from cloud storage to messaging via chat. Many different approaches have also been proposed to provide data protection in the cloud, such as AES, DES, and RSA, but Existing systems often fail when only a certain form of encoding is utilised, either AES, OR DES, OR RSA depending on a consumer requirement. However, the major issue with this scheme is that each encryption is done with encryption keys, and if these keys are leaked in some manner, the entire data is destroyed, so we need a solution that can have additional security. As a result, hybrid cryptography is used in this project, in which current encryption techniques are combined with three new methods. When a user uploads data, it is divided into three sections, the first of which is encrypted with AES, the second with DES, and the third with RSA. LSB steganography is used to store the keys in the image, and the three encrypted files are stored in the cloud. Users must first recover the keys from the image before they can import all data from the server. These keys are then used to decrypt the data once more with AES, DES, and RSA. This approach increases the security of records.**

Keywords—AES, RSA, DES, Hybrid cryptography, LSB, Steganography, Security

I. INTRODUCTION

The present advances are developing at exceptionally quick speed and convey the client with numerous alluring administrations to lessen the weight of huge volumetric information stockpiling and support. These days, numerous online administrations are pertinent which offer a wide range of assistance and information online, for example, e-informing, ebilling, e-exchange, email and so on. Every one These administrations required client's information online for preparation. This information might be any classified data, which is needed by client to be protected from any noxious movement like-medical services data, bank exchange, Visa subtleties, and so on A high necessity emerges for security and insurance of information from any unapproved client as spillage of private data may bring about genuine hindrance to client. This increases the authentication requirement of classified data before transferring it to internet web access.We must build a secure, risk-free mechanism to protect our personal information from such malicious attacks. [6]There is a need to change over classified information into some other structure, which gets peculiar for any assailant and just approved clients can comprehend precisely what information is conveyed. One of the significant procedures to accomplish this prerequisite is cryptography, otherwise called "code making" or "code age". It permits us to make an interpretation of a message into muddled structure for a noxious aggressor. Cryptanalysis and "code cracking" are two other components of this technique.[11]According to the findings, the

Authorized licensed use limited to: Sharda University. Downloaded on September 06,2022 at 06:58:22 UTC from IEEE Xplore. Restrictions apply.

cryptography and steganography concepts mentioned above are very helpful, but the risks of a hacker suspecting that any sensitive or private data is contained in the data being sent are higher.

To keep up security prerequisites, for example, information classification and its honesty, confirmation is an excellent worry to keep any unapproved client from sniffing the information to be imparted between at least two gatherings. To resolve this problem, the owner must first scramble it before transferring it to a cloud specialist company, and only approved clients should be given decoding keys.Presentation of cryptography systems ensures the client information and guarantees that the secret data of the client is shielded and secure from any unapproved client access and malevolent assault. Unapproved client attempts to hamper the client's information by adjusting or altering it. In any case, because of the absence of a key it becomes a monotonous assignment for assailants. Just approved clients have the power and capacity to return the changed information into a unique structure. An effectiveness issue emerges when clients are repudiated and private key encryption won't work all things considered. Cloud information management challenges can be resolved by posing certain concerns such as-

- Distinguishing clients for getting to proprietor secret information.
- Who has the power to alter the current information inside the cloud?
- Will the approved client utilize a similar private key or a one-of-a-kind key allotted to every separate client?
- Where will the keys be stored, and how will the security key(s) be communicated to all authorised clients?
- Which techniques are used to scramble and unscramble cloud data?

From information storage in clouds to enabling messages to be exploited in chat, security is a big concern in a wide range of applications. There square measure numerous techniques for knowledge security in the cloud that are already planned, such as AES, DES, and RSA however, in current strategies the vast majority of time solely exclusive sort of encoding AES, DES, or RSA were used bolstered client demand however, during this system's primary framework downside is every encoding is completed victimization encoding keys on the off chance that these keys area unit disclosed in any case complete knowledge is misplaced thus we need viable method which may offer a lot of security. [9].Both cryptography and steganography are tested in various ways: Steganography does not operate if the "enemy" decodes the contents of the cypher letter; similarly, cryptography fails if the "enemy" discovers the steganographic medium's encoded hidden message.

The DES algorithm established the basis for encryption and presented the first method for implementing and achieving it. While AES data encryption is a more mathematically effective and elegant cryptographic algorithm, its main strength is the ability to use different key lengths. You can choose between 128-bit, 192-bit, or 256-bit keys with AES, making it infinitely stronger. The security of the RSA public-key cryptosystem, which enables encrypted communications and "digital signatures," is based in part on the complexity of factoring large numbers.

Steganography has the advantage of cryptography in that messages do not draw attention to themselves. In places where encryption is illegal, plainly readable encrypted messages, no matter how unbreakable, will arouse suspicion and may be incriminating in and of themselves. The biggest explanation for using the LSB steganography method is that it changes the image as little as possible.

Leakage of keys poses a significant risk to the organisation, exposing it to a variety of internal and external threats. Internal risks include confidential data loss, hacking, legal liability, and data corruption, to name a few. Spyware, malware and Trojan systems are also examples of external threats. To keep the data secret, multiple encryptions are needed.

II. RELATED WORKS

N. Lalithamani and Dr. Soman K. P [1] proposed Cancelable Fingerprint Templates for Irrevocable Cryptographic Key Generation The rising weight of identity fraud has made reliable information management mechanisms a priority in our culture. While protection of information is achieved through a prevalent method as cryptography, it is one of the important issues that must be addressed to secure the secrecy of cryptographic keys. Through integrating biometrics with cryptography, this challenge can be effectively solved. The improved safety efficiency of the cryptographic key has gained a huge reputation among researchers and experimenters.[1] We also propose to use cancelable fingerprint templates to create an irrevocable cryptographic key that works efficiently. The fingerprints are initially used to collect minute points that are effectively converted for the purpose of obtaining deformed points. After that, the deformed points are used to generate cancelable templates used to retrieve irrevocable keys. Because of the fact that the generated key is irrevocable, it's really inefficient to buy cancelled fingerprint models and initial fingerprints.

A. V. Sreedhanya and Dr. Soman K. P Suggested proposal [2] Compressed sensing cryptography's secrecy is a modern imaging system, using both compressive sensing and the scrambling Arnold technique[2]. In a simple linear measurement step, Sparse signal sensing and compression are combined in the compressed sensing (CS) paradigm. With the Arnold Transform, compressed quantities are scrambled. This system also offers better data protection.

Authorized licensed use limited to: Sharda University. Downloaded on September 06,2022 at 06:58:22 UTC from IEEE Xplore. Restrictions apply.

K. N. Sreehari Proposed Symmetric algorithm Efficient key management approaches Key management in encrypted algorithms is an important problem. Key administration comprises generation of keys and the sharing of secret keys between the sender and the receiver. The key should be generated randomly[3]. Sharing the key through a protected channel is also a significant field of science. Various key generation approaches for a symmetrical algorithm are taken into account in this analysis. The lfsr key is used for the first step. For key generation, the second approach is the hash function method.

Bhakthavatchalu R. proposed Implementation of a hybrid cryptographic scheme using DES and MD5 Authenticité, completeness and anonymity during data transfer are provided by cryptographic techniques[4]. A hybrid crypto-system is introduced in this study, which uses both the symmetrical crypto-algorithm and hashing methods. MD5 algorithm is used to determine the hash message value. Using the double DES algorithm, hidden keys will encrypt the same message[4]. Dual DES and hash value ciphertext are mixed and transmitted. On the receiver hand, the text of the cypher is isolated from the hash value.

Suman Kalyan Ghosh proposed Safe and low cost communication hybrid cryptography algorithm Data sharing can lead to sensitive information leakage within a client server architecture or open networks such as the Internet[5]. The aim of encryption is to shield or safeguard data against unwanted access or changes.

S. Joseph Gladwin suggested Hybrid Cryptography and Steganography for Enhanced Security in Suboptimal Images [6], in which they used ECC and Hill cypher. ECC produces the key and uses it to produce the ciphertext. The key is used as the key matrix for the Hill cypher algorithm and generates the ciphertext. Sabyasachi Pramanik [7] used the RSA algorithm to create a private-public key pair. The details in the signature picture are secured using the Sender's Private Key. Encrypted signature header information is embedded in the LSB of blue colour at the sender end. Then, at the LSB of the red colour of the cover image pixels, the pixel detail is embedded. As a result, the stego picture is still available.The encoded information from the stego picture is recovered at the receiver end.

[8]Wassim Alexan presented a method for securely transferring files using AES and steganography techniques, in which they use AES–256 for the cryptographic layer and Least Significant Bit (LSB) encoding for the steganography layer. Cryptography and Steganography Techniques for Multi-facet for Multimedia Data Protection and Hiding suggested by Dr.Ananda Kumar K S,Sinchana M N,Shwetha L Jadav, and Deeraj Naidu [9] used DES encoding and embedded encrypted messages in carrier images using LSB steganography techniques to provide two levels of security for confidential messages.

III. OVERVIEW OF THE SYSTEM

Existing System

- In the current method, the cloud uses some of the encryption methods, and key authentication is performed using the user's information. Various security methods are used depending on the device requirements.
- The authors suggested key link strategies for executing file encryption/decryption and resolving the security issues that must be addressed in cloud storage. They also demonstrated that using a CA inverter and shifter during encryption and decryption, respectively, helps to minimise time complexity and cope with multiple security threats more effectively.

Disadvantages of Existing System

- Because only one encryption technique is used, and keys are not effectively supervised, there is a risk of key leakage.
- AES, DES or RSA methods are used for encryption and the key sharing process is not secure.

Proposed System

To progress Cloud data protection compared to current techniques in which keys are exchanged for protection between users, a new hybrid cryptography technique is proposed, in which three sorts of encryption are utilized: AES, DES and RSA and LSB steganography procedure is utilized to ensure safety for exchange of keys.

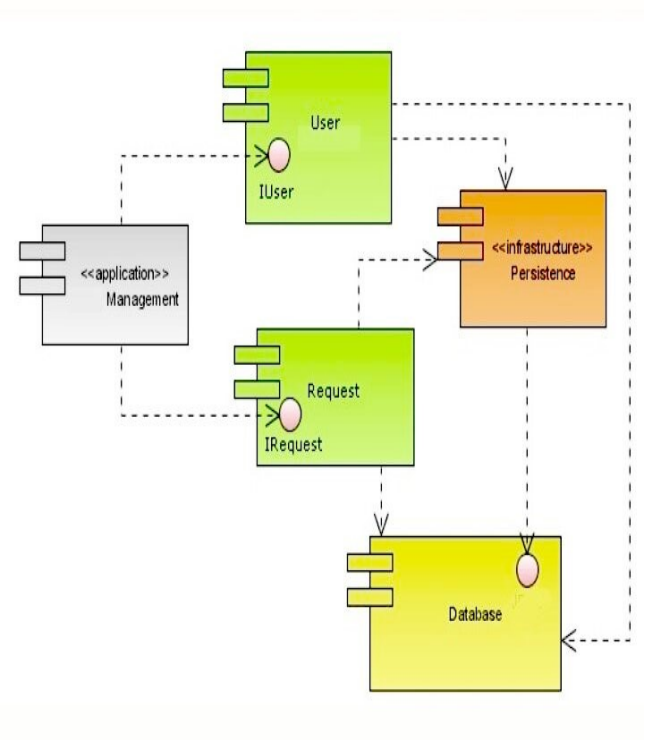

Fig.1 Component Diagram

Authorized licensed use limited to: Sharda University. Downloaded on September 06,2022 at 06:58:22 UTC from IEEE Xplore. Restrictions apply.

As shown in the above Fig.1 The user and request are interfaces imposed by the application. Both the user and request use persistence and DB browser sqlite interfaces. The data in the database is accessed by the user component by utilizing the persistence component in the middleware. Since the persistence is a middleware component , it depends on the database component for data.

Here, IUser, IRequest and DB browser sqlite are the interfaces that are used by the respective components.

Description of proposed system

Firstly, the input Data is divided into three sections, each of which is encoded with a different encoding method, and keys are safely exchanged through incorporating into a picture.Combination of AES, DES and RSA algorithms are used for encrypting one file data. Keys are stored inside the image using LSB algorithm which provides steganography security.

System Modules

In this project work, We used 3 modules and every module has own functions, such as:

1. Owner Module
2. User Module
3. Cloud Module

Owner Module

Owner will register into the application by providing all the necessary details and therefore he/she can login into the application using username and password and the user can upload the files to cloud and share with the other registered users. He/she can also view the files uploaded by him/her and can also view the requests for secret keys from the other users and we can respond and the key will be stored into an image using the lsb algorithm. Using that key, he/she will transfer the file and examine the data.

User Module

User will register with the application and get the username and password. User can see all encrypted files uploaded by all owners and send requests to respective users and get approval to download data and three keys for aes, des, and rsa are shared to the user email which can be used for user download.

Cloud Module

Using cloud module owners can check uploaded encrypted data in a free cloud like drive HQ. Application is connected to cloud server using ftp connection and data is stored by uploading data to cloud.

IV. ALGORITHM

This scheme proposes hybrid encryption, which combines three existing encryption techniques. In this algorithm, the first text file is given as input, and the data is divided into three equal parts by measuring the size of the data and dividing it evenly in three parts, as stated below.

Next data part 1 is given as input to aes encryption algorithm and data is encrypted and keys are stored in the database along with encrypted data. After that part 2 data is encrypted with the DES algorithm and data is encrypted and stored in the database along with keys. Further part 3 data is encrypted with the RSA algorithm and data is encrypted and stored in the database along with keys.

Then the LSB algorithm is used to store three keys in Picture.Lastly to decrypt files, each file is decrypted by sending keys to the mailbox, which are then checked with keys within the image, and if the authentication is successful, the application will ask for a second key. The same procedure is followed for all three passwords, and then the decrypted file is copied.

Hybrid cryptography

Input: text file data
Result: encryption, decryption, splitting, downloading
Txt file=t, image=I; import AES, DES, RSA, LSB library.
File size=f;
Split f/3= f1, f2, f3.
If file ==f1
AES(f1) = aes_encrypt_data.
If file = f2
DES(f2) = des_encrypt_data
If file ==f3
RSA(f3) = rsa_encrypt_data
Get key1, key2, key3

Initialize LSB
LSB (key1, key2, key3) = LSb_to_image

Decryption
LSB = get (key1, key2, key3)

If file ==f1 and key = key1
AES(f1) = aes_decrypt_data.
If file = f2 and key = key2

DES(f2) = des_decrypt_data
If file ==f3 and key = key3

RSA(f3) = rsa_decrypt_data
Get key1, key2, key3

Download (file)

Fig.2 Algorithm

V. EXPERIMENTAL ANALYSIS AND RESULTS

Authorized licensed use limited to: Sharda University. Downloaded on September 06,2022 at 06:58:22 UTC from IEEE Xplore. Restrictions apply.

Table. I Performance Analysis

Input File Size(KB)	Execution Time (Seconds)			
	AES	DES	RSA	HYBRID (AES-DES-RSA)
15	9.0877	4.543859	5.6373	3.954
30	18.17544	9.087718	11.2747	8.632
45	27.2631	13.63158	16.912	13.0021
60	36.35087	18.175	22.549	17.8953
75	45.43859	22.719	28.186	22.20137

As shown in Table I, the planned system needs the least amount of time to execute. as a result of the planned system uses a mixture of bilaterally symmetrical key cryptography algorithms that run at the same time. compared to existing systems, the hybrid algorithmic program takes less time to process text files. In cloud computing, employing a single algorithmic program doesn't give high-level information security.

Anaconda Prompt for ide was used in this project. The admin and user modules' web pages were built using the Python flask platform, html, and CSS. The sqlite database is used in the framework for designing database tables and writing logic in database.py for interaction with all queries with the DB browser.

The proposed model is liable to meet the required security needs of cloud data centers. For data protection, the AES, DES, and RSA algorithms are used. The Proposed system is hybridization of AES,DES and RSA. The concept of separating and combining contributes to the data protection theory. When used in a cloud environment, the hybrid approach allows the remote server to be more stable, allowing cloud providers to gain more user confidence. In terms of data security and privacy protection, the basic difficulty of distinguishing sensitive data and access protection is faced. The following are the different advantages:

The use of public key cryptography facilitates user permission for each file.

The need for a more light and secure encryption system for file information preserving systems on cloud is satisfied.

Because of the data separating and merging, the model is difficult to attack.

VI. CONCLUSION

In the proposed strategy the strength of the AES-DES-RSA mixture increases the degree of security when contrasted with the current procedure where just DES is utilized. In this strategy, the message is encoded with an AES DES RSA, and keys of cipher text are covered up inside a picture utilizing LSB picture steganography. Steganography, exceptionally imparted to cryptography, is a more grounded instrument that permits trading data covertly. With the quick development of advanced innovation and the web, steganography has exceptionally built up a ton in the previous few years. It will test the information on the assailant about both cryptography and steganography. In the event that an aggressor can extract information from the picture, at that point he needs to break the mixture of cryptography then just he will get the specific information. A consequence of the proposed strategy shows that the encryption time is superior to the current procedure. It gives greater security compared with the current one. Savage power assault on this method is hard to use as there is the utilization of AES RSA for DES key.

The picture file is totally stable since it is encrypted with three different encryption algorithms: AES, DES, and RSA.Three Advantages of the implemented procedure is that the key is also safe as it embeds the key in image using LSB and the system is very secure and robust in nature and also Data is kept secured on cloud servers which avoids unauthorized access. The limitations are that it requires an active internet connection to connect with the cloud server and It can be speculated that, despite the increased computational complexity, hybrid cryptographic techniques can accomplish cryptographic goals such as anonymity, integrity, and authenticity. In the future other steganography strategies might be utilized with half breed cryptography for greater security.

VII. FUTURE ENHANCEMENT

In the future we can use this process in a real time cloud environment as of now we are showing with cloud storage only we can use AWS or AZURE real time environment and deploy applications in the cloud and perform hybrid encryption and process data .

REFERENCES

[1] N. Lalithamani and Dr. Soman K. P., “Towards Generating Irrevocable Key for Cryptography from Cancelable Fingerprints”, in Proceedings 2009-2nd IEEE International Conference on Computer Science and Information Technology(ICCSIT 2009)

[2] A. V. Sreedhanya and Dr. Soman K. P., “Secrecy of cryptography with compressed sensing”, Proceedings - 2012 International Conference on Advances in Computing and Communications, ICACC 2012.

[3] K. N. Sreehari, “Efficient key management methods for symmetric cryptographic algorithm”, in 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2018.

[4] K. N. Sreehari and Bhakthavatchalu R., “Implementation of hybrid cryptosystem using DES and MD5”, in 2018 3rd International Conference on Communication and Electronics Systems (ICCES), 2018.

[5] S. K. Ghosh, S. Rana, A. Pansari, J. Hazra and S. Biswas, "Hybrid Cryptography Algorithm For Secure And Low Cost Communication," *2020 International Conference on Computer Science, Engineering and Applications (ICCSEA)*, Gunupur, India, 2020

[6] S. J. Gladwin and P. Lakshmi Gowthami, "Combined Cryptography and Steganography for Enhanced Security in Suboptimal Images," *2020 International Conference on Artificial Intelligence and Signal Processing (AISP)*, Amaravati, India, 2020

[7] S. Pramanik, S. K. Bandyopadhyay and R. Ghosh, "Signature Image Hiding in Color Image using Steganography and

Authorized licensed use limited to: Sharda University. Downloaded on September 06,2022 at 06:58:22 UTC from IEEE Xplore. Restrictions apply.

Cryptography based on Digital Signature Concepts," *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, Bangalore, India, 2020

[8] W. Alexan, A. Hamza and H. Medhat, "An AES Double–Layer Based Message Security Scheme," 2019 International Conference on Innovative Trends in Computer Engineering (ITCE), Aswan, Egypt, 2019

[9] D. Naidu, A. K. K S, S. L. Jadav and M. N. Sinchana, "Multilayer Security in Protecting and Hiding Multimedia Data using Cryptography and Steganography Techniques," *2019 4th International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT)*, Bangalore, India, 2019

[10] Z. F. Yaseen and A. A. Kareem, "Image Steganography Based on Hybrid Edge Detector to Hide Encrypted Image using Vernam Algorithm," *2019 2nd Scientific Conference of Computer Sciences (SCCS)*, Baghdad, Iraq, 2019

[11] K. Manjula Shenoy and S. G. Shaikh, "An Approach to Secure Data Transmission Through the Use of Cryptography and Steganography," *2019 International Conference on Communication and Electronics Systems (ICCES)*, Coimbatore, India, 2019

[12] A. Mendhe, D. K. Gupta and K. P. Sharma, "Secure QR-Code Based Message Sharing System Using Cryptography and Steganography," *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, Jalandhar, India, 2018

[13] H. Arora, C. Bansal and S. Dagar, "Comparative study of image steganography techniques," *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, Greater Noida, India, 2018

[14] G. R. J. and R. S. Ganesh, "Review of Recent Strategies in Cryptography-Steganography Based Security Techniques," *2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET)*, Kottayam, India, 2018

[15] S. S. More, A. Mudrale and S. Raut, "Secure Transaction System using Collective Approach of Steganography and Visual Cryptography," *2018 International Conference on Smart City and Emerging Technology (ICSCET)*, Mumbai, India, 2018

Authorized licensed use limited to: Sharda University. Downloaded on September 06,2022 at 06:58:22 UTC from IEEE Xplore. Restrictions apply.