Secure File Storage on the cloud Using Hybrid Cryptography

SHALIN DASHORA
Minor Project III
Chandigarh University
Punjab, India
shalindashora08@hotmail.com

NAVNEET GUPTA
Minor Project III
Chandigarh University
Punjab, India
navneetguptaend@gmail.com

MILIND PAL SINGH TANWAR
Minor Project III
Chandigarh University
Punjab, India
milindpalsingh1@gmail.com

ABHINAV SINGH
Minor Project III
Chandigarh University
Punjab, India
absingh.singh21@gmail.com

RAMNEET KAUR
Minor Project III
Chandigarh University
Punjab, India
ramneet.e13422@cumail.com

***Abstract*— Secure file storage in a hybrid cloud using cryptography refers to the process of ensuring that files stored in a hybrid cloud environment are secure from unauthorized access, tampering, or theft. Hybrid cloud refers to a cloud computing environment that combines on-premises infrastructure with one or more public or private cloud providers. Cryptography is used to secure the files in transit and at rest. Cryptography involves the use of mathematical algorithms and protocols to ensure that data is protected from unauthorized access[1]. This includes encryption, which converts the original data into an unreadable format, and decryption, which converts the encrypted data back to its original format. Overall, secure file storage in hybrid cloud using cryptography [3] is essential for protecting sensitive data and ensuring that it remains secure, even in a cloud computing environment. It requires a comprehensive approach that includes strong encryption, secure transmission, and robust access controls.**

Keywords*— *Cryptography, Confidentiality, Integrity, Availability, Storage, and Security.

I. INTRODUCTION

The aim of the project is to create an encrypted and secured file storage system to transfer files to users in a remote location. This system will require an input that is successfully encrypted using any of the algorithm techniques and stored anywhere. The uploaded file can be downloaded by other users, but to read the data present in it, they have to decrypt the file using the decryption algorithm and the information provided about the file within the users by the owner. The system uses public-key cryptographic techniques like RSA and Symmetric key cryptography like AES. Hashing techniques like static hashing and dynamic hashing are used for performing integrity. Due to the encryption of data, confidentiality is also achieved in the process. The project is also open to new challenges and future changes to other advanced technologies in keeping the data secured. The system we propose is to divide the file storage process into three parts which use the three encryption techniques of DES [4], AES [5], and, RSA[7] in succession thus providing an overall advanced secure and trustable file storage system in the cloud using the cryptography methods in hybrid. In this project, three novel technologies are integrated with existing encryption methods to generate hybrid cryptography.

Data is split into three portions when a user uploads it, with the first section using AES encryption, the second using DES encryption, and the third using RSA encryption. The three encrypted files are saved on the cloud, and the keys are concealed in the image using LSB steganography. Before importing all of the server's data, users must first recover the keys from the image. The data is subsequently decrypted once again using RSA, DES, and AES using these keys. This strategy improves record security.

II. LITERATURE REVIEW

TABLE 1. REFERENCE TO PAPERS

Article/ Author	Year and Citation	Tools/ Software	Technique	Evaluation Parameter
Rashi Dhagat, Purvi Joshi [6]	2016	VS-Code, Python Interpreter	Public key exchange (PKA)	Encryption technique
Punam V Maitri, Aruna Verma [8]	2016	VS-Code, Python Interpreter	AES, Blowfish, RC6 algorithm.	Encryption technique
Jerzy Kaczmarek, Michał Wróbel [9]	2008	VS-Code, Python Interpreter	Cryptographic hash functions	Encryption technique
M. Malarvizhi, J. Angela Jennifa Sujana, T. Revathi [11]	2014	VS-Code, Python Interpreter	AES, Blowfish, RC6 algorithm	Encryption technique
P. Bharathi, S. Rajashree [12]	2014	VS-Code, Python Interpreter	Third Party Auditor (TPA)	Encryption technique
Punam V. Maitri, Aruna Verma [13]	2016	VS-Code, Python Interpreter	AES, Blowfish, RC6 and BRA	Encryption technique
Rohit Barvekar, Shrajal Behere, Yash Pounikar, Anushka Gulhane [15]	2018	VS-Code, Python Interpreter	AES, Blowfish, RC6	Cryptographic Algorithms

III. EXISTING SYSTEM

Existing systems are currently concerned with the usage of only one or a combination of a few of the techniques which could provide time for the attacks to hack into the file content. But this would only delay the attack and not prevent it and thus the security is compromised.

DES (Data Encryption Standard) encrypts plain text with a 56-bit key, making it simple to decrypt with the aid of contemporary technology. Due to the meet-in-the-middle attack, which may be used to defeat double DES, double DES only provides security level 256 rather than 2112, while using a 112-bit key.

Due to the meet-in-the-middle attack vulnerability, Triple DES uses a 168-bit key but provides a total security level of 2112 bits instead. Because of the small block size and usage of the same key to encrypt huge amounts of information, block collision attacks and sweet32 attacks are also possible.

The fact that AES is a symmetric algorithm and necessitates the use of the same key by both the encryptor and the decryptor is a significant drawback. The all-important secret key cannot be disseminated to maybe hundreds of recipients worldwide without facing the significant danger of it being accidentally or purposefully compromised somewhere along the road, which raises a fundamental key management problem. Combining the benefits of DES, AES, and RSA encryption is the answer.

IV. PROPOSED SYSTEM

The system we propose is to divide the file storage process into three parts which uses the three encryption techniques of DES, AES, and RSS in succession thus providing overall advanced secure and trustable file storage system in the cloud using the cryptography methods in hybrid.

In this project, three novel technologies are integrated with existing encryption methods to generate hybrid cryptography. Data is split into three portions when a user uploads it, with the first section using AES encryption, the second using DES encryption, and the third using RSA encryption. The three encrypted files are saved on the cloud, and the keys are concealed in the image using LSB steganography. Before importing all of the server's data, users must first recover the keys from the image. The data is subsequently decrypted once again using RSA, DES, and AES using these keys. This strategy improves record security.

Authorized receivers publish a public key while holding onto an accompanying private key that only they are aware of in order to obtain the secret key needed to decode that material. The sender then encrypts and sends each receiver their unique secret AES key, which can be used to decode the material, using that public key and RSA.

V. METHODOLOGY

Modern cryptographic algorithms can be implemented using dedicated cryptographic hardware or software running on general-purpose hardware. For various reasons, dedicated cryptographic hardware provides a better solution for most applications. Table 1 shows a list of reasons hardware-based cryptographic solutions are more desirable.

TABLE 2. IMPLEMENTATION TECHNIQUES

Hardware Based Cryptography	**Software Based Cryptography**
Uses dedicated hardware thus much faster to execute.	Uses shared hardware thus slower to execute.
Not dependent on the operating system. Supported by dedicated software for operating the hardware.	Dependent on the security levels and features of the operating system and supported software.
Dependent on the security levels and features of the operating system and supported software.	No dedicated secure memory locations available. Thus, susceptible to stealing or manipulation of keys and data.
Maxim hardware implementations have protections built in against reverse engineering such as PUF (ChipDNA).	Software implementations can be easier to reverse engineer.
In a hardware system, special care is taken to hide and protect the vital information such as private keys to make it much more difficult to access	In a general-purpose system where software cryptography is implemented, there are more ways to snoop and access to vital information. An example would be intercepting the private key in transit within the computer's system.

Constraint Identification:

1. Data-in-transit

Data that is travelling between endpoints is called data-in-transit. When using an internet browser, you may observe one general type of data-in-transit cloud encryption: the HTTPS and HTTP protocols which secure the information channel you use when visiting websites on the internet. They achieve this by enclosing a secure channel in an encryption layer called an SSL, or “Secure Socket Layer.”

The SSL inside HTTP or HTTPS encrypts the data exchanged between your endpoint and the endpoint for the website you are viewing so that the hacker can only view encrypted data when your channel is compromised.

2. Data-at-rest

Sensitive information is kept in business IT systems like servers, discs, or cloud storage services. You can implement access control by encrypting data while it is being kept and distributing decryption keys only to authorized personnel. Plaintext information won’t be visible to anyone attempting to access your data-at-rest; instead, encrypted data will. Manufacturers of hard drives are now providing self-encrypting devices that adhere to trusted storage criteria for cloud cryptography. Drives with built-in encryption circuitry provide automated encryption at a low cost and with little performance.

3. Legal and regulatory issues

Each client must have its legal and regulatory experts examine the policies and practices of the cloud provider to assess their suitability to confirm that it has rules and practices that address legal and regulatory challenges. Data security and export, compliance, auditing, data retention and destruction, and legal discovery are the factors to be considered. Trusted Storage and TPM access approaches can be quite effective at limiting access to data in the areas of deletion and retention.

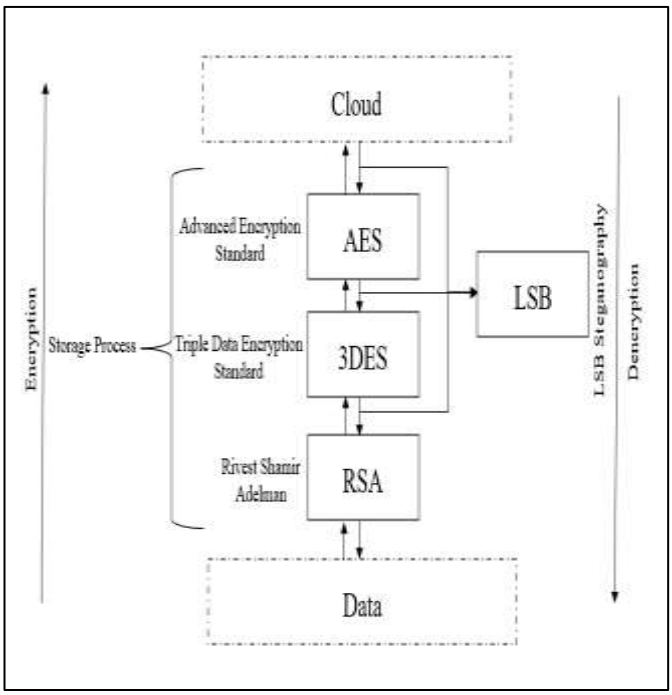
4. Authentication

The mainstay of access control is often user authentication, which keeps the bad guys out while facilitating easy access for authorized users. Since the cloud and all of its data are accessible to anyone over the internet, authentication and access control are more crucial than ever in the cloud context.

5. Customer Separation

One of the most obvious cloud security concerns is segregating users of a cloud provider (who may be rival businesses or even hackers) to prevent accidental or deliberate access to critical data. A cloud provider uses virtual machines and hypervisors to divide their clients. Technologies for cloud cryptography can significantly boost the security of VM and network isolation.

The system focuses on storing files in cloud using hybrid cryptography that secures the data at rest through a software application with codes of crypto and stegano- algorithms that can be incorporated into any OS, System application, API, interfaces, etc.



Working

VI. COMPONENTS EXPLANATION

By encrypting data stored in the cloud, cloud cryptography extends the same level of security to cloud services. Without slowing down data transfer, it can protect sensitive cloud data. Many firms create cryptographic protocols to maintain a balance between security and efficiency in their cloud computing. The following cryptography formulas are employed for cloud security:

1. Symmetric Algorithm:

This encryption technique removes the need for manual encryption and decryption by enabling authorized users to access data at rest and while in transit. The approach automatically encrypts important information whenever login credentials are given. One key is used for both information decoding and encryption. It operates at a very high level of encryption and doesn't need a lot of computer resources. Two-way keys are used in symmetrical algorithms to ensure validation and approval. The encrypted data is stored in the Cloud and cannot be decrypted unless the client knows the key.

- Standard for Advanced Encryption (AES)
- Common Data Encryption (DES)

2. Asymmetric Algorithm

Different kinds of keys are used for encryption and decryption in asymmetric algorithms. Each recipient of this type needs a decryption key. The recipient's private key is another name for this key. Typically, a particular individual or an organization is the owner of the encryption key. Since it requires both keys to access particular information, this algorithm is considered the safest.

- Rivest Shamir Adleman Algorithm (RSA)
- Elliptic Curve Cryptography (ECC)

As per the methodology we divide the file storage process into three parts: DES, AES, and RSS in succession with LSB steganography key management, providing overall advanced secure file storage system in the cloud.

A. AES

The Advanced Encryption Standard (AES) is the trusted standard algorithm used by the United States government and other organizations. Although extremely efficient in the 128-bit form, AES also uses 192- and 256-bit keys for very demanding encryption purposes. AES is widely considered invulnerable to all attacks except for brute force. Regardless, many internet security experts believe AES will eventually be regarded as the go-to standard for encrypting data in the private sector.

B. Triple DES

Triple DES is the successor to the original Data Encryption Standard (DES) algorithm, created in response to hackers who figured out how to breach DES. This is because the 3DES method encrypts its data three times with the Data Encryption Standard (DES) cypher. DES is a Feistel network-based

symmetric-key technique.

As a symmetric key cypher, it employs the same key for both encryption and decryption. The Feistel network renders each of these processes almost identical, resulting in a more efficient technique to implement. Although DES has a 64-bit block and key size, the key only provides 56 bits of protection in practice. Because of the short key length of DES, 3DES was created as a more secure alternative. The DES algorithm is executed three times with three keys in 3DES; nevertheless, it is only deemed secure if three distinct keys are utilized. TripleDES applies the DES algorithm three times to every data block and is commonly used to encrypt UNIX passwords and ATM PINs.

- EMV payment systems
- Microsoft Office
- Firefox

C. RSA

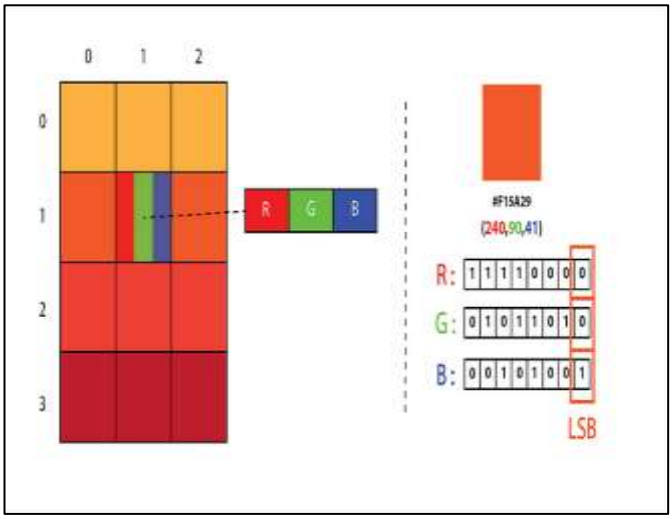
RSA is a public-key encryption asymmetric algorithm and the standard for encrypting information transmitted via the internet. RSA encryption is robust and reliable because it creates a massive bunch of gibberish that frustrates would-be hackers, causing them to expend a lot of time and energy to crack into systems.

Rivest-Shamir-Adleman (RSA)- Rivest-Shamir-Adleman is an asymmetric encryption algorithm that works off the factorization of the product of two large prime numbers. Only a user with knowledge of these two numbers can decode the message successfully. Digital signatures commonly use RSA, but the algorithm slows down when it encrypts large volumes of data.

D. LSB IMAGE STEGANOGRAPHY

LSB [14] Steganography is an image steganography technique in which messages are hidden inside an image by replacing each pixel's least significant bit with the bits of the message to be hidden.

Considering a digital image to be a 2D array of pixels. Each pixel contains values depending on its type and depth. We will consider the most widely used modes — RGB(3x8-bit pixels, true-color) and RGBA(4x8-bit pixels, true-color with transparency mask). These values range from 0–255, (8-bit values).



Representation of Image as a 2D Array of RGB Pixels

We can convert the message into decimal values and then into binary, by using the ASCII Table. Then, we iterate over the pixel values one by one, after converting them to binary, we replace each least significant bit with that message bits in a sequence.

To decode an encoded image, we simply reverse the process. Collect and store the last bits of each pixel then split them into groups of 8 and convert it back to ASCII characters to get the hidden message.

TABLE 3. COMPARISON OF CRYPTOGRAPHIC ALGORITHMS USED IN HYBRID

Factors	AES	DES	RSA
Designed by	Vincent Rijmen, Joan Daemen , 2001	IBM, 1975	Ron Rivest, Adi Shamir, and Leonard Adleman, 1978
Key Length	128,192,256 bits	56 bits	>1024 bits
Cipher Block Size	Size of 128 bits	Size of 64 bits	Min 512 bits
Scalable	No	Yes	No
Algorithm Type	Symmetric Key	Symmetric Key	Asymmetric Key
Encryption Time	Fast	Medium	Slow
Decryption Time	Fast	Medium	Slow
Power Utilization	Less	Less	Very High
Security efficiency	Highly Secured	Secured Moderately	Least Secure
Key Usage for Encrypt & Decrypt	Uses Same Key	Uses Same Key	Different Key
Number of Rounds	10\12\14 Rounds	16 Rounds	Single Round
Simulating Speed	Fast	Fast	Fast
Hardware & Software	Fast	Better implementation of Hardware than Software	Less Efficient

VII. CONCLUSION AND FUTUREWORKS

In conclusion, secure file storage in the cloud using hybrid cryptography is essential for protecting sensitive data and ensuring that it remains secure, even in a cloud computing environment. The proposed system offers a more robust and secure file storage solution by combining three encryption techniques and hashing techniques for integrity. The system also ensures confidentiality by encrypting data in transit and at rest.

The proposed system can be further improved by incorporating new technologies to enhance security, such as multi-factor authentication, intrusion detection, and prevention systems, and security analytics. The system can also be tested using various attack scenarios to evaluate its effectiveness and ensure that it can withstand attacks from potential adversaries. Overall, the proposed system provides a solid foundation for

secure file storage in the cloud using cryptography.

Applications of Cryptographic algorithms are discussed below:

- Secure communication
- Data protection
- Secure communication
- Authentication
- Secure storage
- Digital currencies
- Military applications

There are various opportunities for future research in this sector. To begin, the suggested system may be enhanced by including more powerful encryption and steganography methods. Second, the system may be expanded to provide for multi-user access and collaboration, allowing numerous users to securely upload, share, and collaborate on content. Third, several criteria such as reaction time, scalability, and efficiency may be used to evaluate the system. Finally, to evaluate its resilience and efficacy, the proposed system may be evaluated against various sorts of assaults such as brute-force attacks, denial-of-service attacks, and man-in-the-middle attacks. Overall, the suggested system offers a lot of future research and development potential in the field of secure file storage in a hybrid cloud employing cryptography.

ACKNOWLEDGMENT

The success and final result of this project necessitated a great deal of support and assistance from many people, and we consider ourselves incredibly fortunate to have received it during the duration of my project. Much of what we've accomplished has been possible only because of their guidance and assistance, and we'd like to express our gratitude to them. The authors immensely thank Ms. Ramneet Kaur, teacher in charge, Minor Project III, Chandigarh University, Punjab, India, for her full support extended to carry out this research.

REFERENCES

1. N. Lalithamani and Soman K. P., "Towards Generating Irrevocable Key for Cryptography from Cancelable Fingerprints", Proceedings 2009–2nd IEEE International Conference on Computer Science and Information Tsechnology (ICCSIT 2009).

2. A. V. Sreedhanya and 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", 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", 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), 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 SirrnaI Processing-(AISP), 2020.

7. S. Pramanik, S. K. Bandyopadhyay and R. Ghosh, "Signature Image Hiding in Color Image using Steganography and Cryptography based on Digital Signature Concepts", 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), 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 (IT CE), 2019.

9. D. Naidu, A. K. KS, 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), 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), 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), 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), 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), 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), 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), 2018