"Cipher Nest: Secure File Storage usingHybrid Cryptography"

Mr. Chintan Jethva
Electronics and Telecommunication
Vivekanand Education Society's Institute of Technology
Mumbai, India

Dhwani Panchal
Electronics and Telecommunication
Vivekanand Education Society's Institute of Technology
Mumbai, India

Priyal Singh
Electronics and Telecommunication
Vivekanand Education Society's Institute of Technology
Mumbai, India

Manasi Pawar
Electronics and Telecommunication
Vivekanand Education Society's Institute of Technology
Mumbai, India

Aniket Sangle
Electronics and Telecommunication
Vivekanand Education Society's Institute of Technology
Mumbai, India

***Abstract*— In the modern era of digital communication and information exchange, ensuring the confidentiality and integrity of sensitive data has become paramount. Cryptography plays a pivotal role in safeguarding information through the use of encryption and decryption techniques. This paper provides a comprehensive overview of encryption and decryption methods in cryptography. The core of the paper delves into the basic cryptographic building blocks, covering symmetric and asymmetric encryption algorithms. Symmetric algorithms, such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES), use a single secret key for both encryption and decryption. Asymmetric algorithms, exemplified by Rivest–Shamir–Adleman (RSA) employ pairs of public and private keys, enhancing security and key distribution.**

***Index Terms*—Cryptography, RSA, AES, Triple DES**

I. INTRODUCTION

In the contemporary era, the vast majority of individuals prioritize the exchange of data via the internet and mobile storage devices. However, a significant portion neglects to encrypt their data, despite being aware of its sensitive nature and the heightened risk of loss or unauthorized access. Ensuring information security is paramount across all spheres of life, particularly as technology increasingly governs daily operations. Cryptography serves as a crucial tool in safeguarding data during transmission, rendering it indecipherable to unauthorized parties. The overarching goal of this initiative is to enhance both AES and RSA algorithms to achieve low power consumption, high throughput, real-time processing, reliability, and exceptional security.

In recent years, cloud computing has emerged as a revolutionary paradigm, transforming the way data is stored, accessed, and managed. The cloud offers unparalleled convenience and scalability, enabling individuals and organizations to effortlessly store and retrieve their digital assets. However, this convenience comes with a critical caveat – the security and confidentiality of sensitive data. As more and more critical information is entrusted to cloud service providers, ensuring the robust protection of files against unauthorized access and cyber threats becomes a paramount concern. Traditional encryption methods, while effective, may not provide a holistic solution to the evolving challenges posed by an increasingly sophisticated threat landscape. Asymmetric encryption offers robust security but can be computationally intensive for large datasets. Symmetric encryption is efficient but presents challenges in secure key distribution and management. In response to these limitations, hybrid cryptography has emerged as a compelling approach that leverages the strengths of both symmetric and asymmetric encryptions to create a unified and formidable defense against potential security breaches.

Cryptography encompasses a range of techniques and algorithms aimed at achieving diverse security goals. The primary classifications within cryptography are symmetric-key cryptography and asymmetric-key cryptography. Here's an overview of these types:

A. Symmetric key Cryptography

Symmetric-key cryptography, alternatively referred to as a secret-key or a private-key cryptography, employs a single secret key for both encrypting and decrypting cipher text. The confidentiality of this shared key is paramount and must be maintained between the parties involved in communication. Widely utilized across numerous applications, symetric key cryptography ensures data confidentiality effectively.

B. Asymmetric Key Cryptography:

Asymmetric-key cryptography, also known as public-key cryptography, is a cryptographic technique that uses a pairof mathematically related, but distinct, keys for encryptionand decryption. One key is designated as the public key, and the other as the private key. The public key can be freely distributed,while the private key must be kept secret. This approach enables various security features and applications including securedata transmission, digital

signatures, and key exchange.

II. Security Challenges

When data is not encrypted, it is vulnerable to various security challenges and risks. Encryption serves as a fundamental mechanism for protecting sensitive information from unauthorized access, interception, and manipulation. Here are some security challenges associated with the absence of encryption:

A. Unauthorized Access:

Without encryption, data is exposed to unauthorized access. Anyone with access to the network or storage where the data resides can potentially view and exploit the information.

B. Data Tampering

In the absence of encryption, malicious actors can modify or tamper with the data without detection. This poses a risk to the integrity of the information, as altered data may lead to inaccurate decision-making or compromise the reliability of systems.

C. Confidentiality Breach

Sensitive and confidential information, such as personal identifiable information (PII), financial data, or trade secrets, is at risk of exposure if not encrypted. Unauthorized individuals or entities may exploit this information for malicious purposes including identity theft or corporate espionage.

D. Risk during Transmission

Unencrypted data transmission, especially over unsecured networks, exposes the data to interception and eavesdropping. This risk is particularly significant in public Wi-Fi or other shared network environments.

To address these challenges, encryption should be implemented as part of a comprehensive security strategy. Employing strong encryption algorithms, securing data in transit and at rest, and adhering to best practices in key management are crucial steps in mitigating the risks associated with the lack of encryption.

III. Literature Review

Secure File Storage on Cloud Using Hybrid Cryptography: The project highlights the substantial security apprehensions among data owners when entrusting their information to cloud platforms. The research concludes with the development of a secure system boasting enhanced data integrity, heightened security measures, minimized latency, and strengthened confidentiality. However, it's noted that the BLOWFISH algorithm lacks authentication and non-repudiation capabilities when two parties share the same key.

A security model to protect the isolation of medical data in the cloud using hybrid cryptography: The architecture facilitates data distribution based on contractual agreements and provides on-demand access to various services via the internet. To bolster security, the Mackey-glass equation, coupled with the RKO method, is integrated, along with optimized key selection utilizing the DES algorithm. Nevertheless, DES's susceptibility to brute-force attacks, particularly with its 56-bit key, renders it inadequate for software applications and may result in sluggish performance. of 56-bit key as brute-force attack can devastate it easily. This algorithm is not efficient for software's and runs slowly on software's.

Scalable CCA-secure public-key authenticated encryption with keyword search from ideal lattices in cloud computing. The proposal introduces a novel concept of public-key encryption with keyword search (PEKS), allowing efficient and secure data retrieval from encrypted data sets. This scheme boasts quantum-resistant properties, along with IKGA and IND-CCA security, suitable for conjunctive keyword searches and multi-user scenarios. However, the larger sizes of ciphertexts and tokens compared to similar schemes incur computational memory costs.

Research on cloud data encryption algorithm based on bidirectional activation neural network: The study enhances data security through a newly devised bidirectional activation (BA) neural network, which conceals the original encryption key used in cloud-based encryption. While this approach fortifies key security against brute-force attacks, its adaptability in encryption remains limited.

Research Gap

Unlike prior works utilizing BLOWFISH and DES algorithms, proposed system employs AES and RSA algorithms, known for their efficiency, real-time processing, reliability, and robust security. Moreover, the proposed system demonstrates higher adaptability and reduced storage space requirements for cipher keys compared to previous research. However, it's noted that the simplicity of the utilized algorithms may necessitate enhancements for more sophisticated applications. Additionally, the utilization of Python in the proposed system streamlines algorithm implementation without sacrificing speed.

IV. Algorithms

A. Advanced Encryption Standard (AES)

AES, a symmetric-key encryption algorithm, is widely acclaimed for securing sensitive data across various applications. With key sizes of 128, 192, or 256 bits, AES offers enhanced security proportional to the key length, effectively withstanding cryptanalysis and earning widespread trust globally**.**

B. RSA (Rivest–Shamir–Adleman)

RSA, an asymmetric-key encryption algorithm, serves to secure data transmission and digital signatures. Operating with a public-private key pair, RSA encrypts data with the public key, decryptable solely with the corresponding private key.

C. Triple DES (Data Encryption Standard)

Triple DES (Data Encryption Standard) is a symmetric-key block cipher algorithm that applies the DES algorithm three times to each data block. Also known as 3DES or TDES, it was introduced as a way to increase the key size of DES to enhance security. DES, the predecessor to 3DES, uses a 56- bit key, which was considered secure in its early yearsbut became vulnerable to brute-force attacks as computational power increased. ripple DES supports different keying options, including two-key (K1, K2) and three-key (K1, K2, K3) options. In two-key triple DES, the first and third stages use thesame key (K1 and K3), while the second stage uses a differentkey (K2). In three-key triple DES, each stage uses a different key (K1, K2, K3). Like DES, Triple DES operates on64-bit blocks of data.

D. Ascon

Ascon is a lightweight authenticated encryption algorithm designed for securing data in constrained environments, such as low-power devices and embedded systems. The name" As- con" derived from the Latin word" ascender," meaning" to rise," its suitability for lightweight and resource-constrained applications. Ascon was one of the candidates in the CAESAR competition (Competition for Authenticated Encryption: Security, Applicability, and Robustness), which aimed to select new authenticated encryption algorithms.

V. PROPOSED SYSTEM

In this project two algorithms are used and are compared

A. AES

1. Key Expansion: AES functions with a constant block size of 128 bits (16 bytes). Tailored to the selected key size (128, 192, or 256 bits), AES utilizes key expansion algorithms to transform the original key into a comprehensive key schedule. This schedule produces a sequence of round keys derived from the initial key.
2. Initial Round Key Addition: The input plaintext data is segmented into 128-bit blocks. Employing a bitwise XOR (Exclusive OR) operation, the initial round key is combined with the plaintext.
3. Rounds: AES conducts multiple encryption rounds (10, 12, or 14 rounds, contingent on the key size). Each round encompasses various transformation stages: Sub-bytes: Byte substitution is executed utilizing a predefined substitution table (S-box). ShiftRows: The rows of the block undergo cyclic shifting. MixColumns: Column mixing within the block is performed via matrix multiplication. AddRoundKey: A round key derived from the expanded key schedule is incorporated. Final Round: The final round bears resemblance to preceding rounds but excludes the MixColumns stage. Following this final round, the encrypted data (cipher text) is derived.
4. Security: AES is designed to be secure against various cryptographic attacks. The strength of AES depends on keysize used (128, 192, or 256 bits). Brute force attacks on AES encryption are computationally infeasible due to large key space.

B. Triple DES

1. Keying Options: Triple DES operates with different keying options: 2-key Triple DES and 3-key Triple DES. In 2- key Triple DES, three keys (K1, K2, K1) are used, where K1 and K2 are independent keys. In 3-key Triple DES, threedifferent keys (K1, K2, K3) are used.
2. Encryption Process: Encryption Process: Triple DES carries out encryption through a series of iterations, typically employing blocks of 64 bits. The encryption process unfolds in the following sequence: Initial Permutation (IP): At the outset, the input block undergoes an initial permutation, a crucial step in the encryption process aimed at rearranging the bits within the block. Round 1: In this stage, the initial block undergoes encryption using the first key (K1) in the Triple DES sequence. This operation involves applying complex mathematical transformations to the block, guided by the specific key. Round 2: Following Round 1, the result obtained is subjected to decryption, utilizing the second key in the Triple DES sequence. This decryption step is integral to the Triple DES process, as it ensures multiple layers of security by introducing a different key for subsequent operations. This multi-round encryption procedure, coupled with the intricate permutations and transformations applied at each stage, collectively fortifies the security of the Triple DES encryption scheme.
3. Security: Triple DES is considered more secure than the original DES due to the increased key size (168 bits for 3-key mode). However, due to advancements in computing power, Triple DES with a 56-bit effective key length (in 2-key mode) is now considered relatively weak for modern security standards. Advanced encryption standards like AES are preferred for new encryption implementations due to their stronger security properties.

VI. IMPLEMENTATION AND RESULTS

The proposed system was built using python. A file was encrypted successfully and after encrypting a user can view the encrypted file and can send to the client.

The proposed system cannot be hacked or corrupt the important and confidential data. The proposed system uses AES and Triple DES algorithms. The proposed system performance were compared with existing system and the following results were obtained. Encryption time is considered for both algorithms.

Table no 1 comparison of time:

File size	AES Algorithm	Triple DES Algorithm
500 KB	0.00711	0.0264058
10 MB	0.0645163	0.5513
102 MB	0.037452	0.6533145

A line graph and bar graph is presented below for better understanding

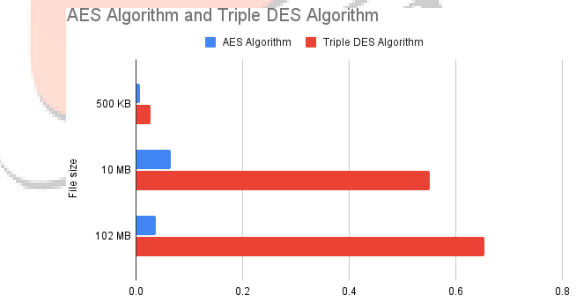

Fig. 1. Time taken by AES and Triple DES

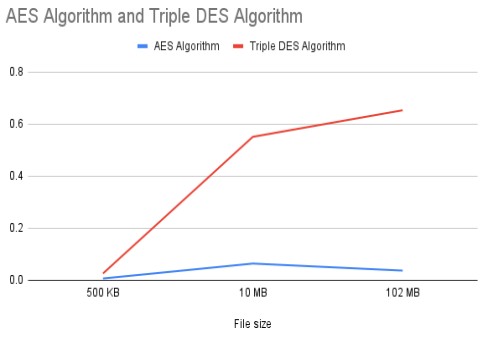

Fig. 2. Time taken by AES vs Triple DES

VIII. CONCLUSION

In summary, the comparison between AES and Triple DES algorithms reveal that AES generally offers faster encryption speeds across various file sizes. While AES demonstrates superior efficiency, Triple DES may still be relevant for certain applications due to factors like backward compatibility. However, the choice between the two ultimately depends on specific security and performance requirements. Understanding these trade-offs aids in making informed decisions regarding encryption algorithm selection for different use cases.

IX. REFERENCES

[1] Shrikanta Jogar, Darshan Handral, Secure File Storage on Cloud using Hybrid Cryptography, Volume 2, Issue 2,
IJARSCT, July 2023

[2] Swetha Gadde, J. Amutharaj, S. Usha, A security model to protect the isolation of medical data in the cloud using hybrid cryptography, Journal of Information Security and Applications, Volume 73, 2023

[3] Lish Yao, Jian Weng, Anjia Yang, Xiaojian Liang, Zhenghao Wu, Zike Jiang, Lin Hou, Scalable CCA-secure public-key authenticated encryption with keyword search from ideal lattices in cloud computing, Information Sciences,
Volume 624, 2023

[4] Zhenong Man, Jinqing Li, Xiaoqiang Di, Ripei Zhang, Xusheng Li, Xiaohan Sun, Research on cloud data encryption algorithm based on bidirectional activation neural network, Information Sciences, Volume 622, 2023,