The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1979 – 1988

Comparative analysis of enhanced hybrid encryption algorithm with single encryption algorithm

Renuka S. Durge[1] and Vaishali M. Deshmukh [2]

Computer Science and Engineering, Sant Gadge baba Amravati University, Amravati, India.

renuka434@gmail.com[1] , vmdeshmukh@mitra.ac.in[2]

Abstract - To accomplish end users data security, it appears that the methods currently used to ensure data security, privacy, integrity, and availability to cloud users are insufficient. An encryption method will be required to guarantee the private preservation of users data while it is in transit or persistent state. The security of cloud data is ensured by a hybrid encryption algorithm that includes the use of the symmetric Advanced Encryption Standard (AES) and an asymmetric RSA algorithm ,combining an asymmetric algorithm (public-key cryptography, or PKC) with a symmetric algorithm (also called private key cryptography), which employs a single key for encryption and decryption, to increase the security of cloud data. Hybird encryption has significant benefits over single encryption in terms of security, speed and computation time. By first encrypting data with AES and then encrypting the AES key with RSA while in the cloud, the suggested method offers a hybrid encryption scheme that improves the security of cloud data. This paper examines various forms of cryptographic encryption and also offers a enchanced hybrid encryption technique for online applications.

Keywords : Hybrid Encryption; Advanced Encryption Standard; RSA; Cryptography.

I.Introduction

Today's society is based on computer networks, which have evolved into its foundation. The extent to which people rely on the network is comparable to that of necessities like electricity, water, etc. Personal, professional, and social data are quickly transmitted, processed, and used by the network. People's social and family lives are supported in every way possible by the network. There are unexpected issues with assets, character, training, and, surprisingly, the whole friendly design. Data stored in cyberspace can

be easily transferred, processed, and shared, but it is difficult to control. The need to protect privacy information is becoming more and more pressing as a result of high-risk issues like misuse, tampering, and impersonating other people. Despite the fact that cyberspace makes life easier for people, it also has some drawbacks, such as the leakage of trade secrets

and personal data.[1] Cryptography algorithms can be used to protect data from snoopers and ensure the security of cloud data using a hybrid encryption that combines symmetric algorithm and asymmetric algorithms.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1979 – 1988

II. Methods and Materials

2.1 Software and Algorithms:

The best answer is to build cryptosystems under the presumption that data will leak.as depicted in Figure 1. In order to keep systems secure even when the underlying circuits might leak information, Cryptography Research has created methods for securing current cryptographic algorithms (such as RSA, AES, DES, and Elliptic Curve systems). The leak reduction and masking methods are also necessary when the physical hardware leaks excessively.

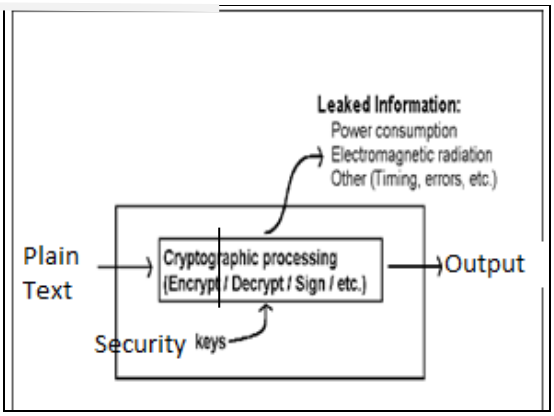

Fig.1 AES Attacks

a) Analysis of power: attacks in which the hardware uses varying amounts of power for computation.

b) Attack Time: assaults in light of estimating what amount of time different calculations require to perform.

c) Attack of fault: in which flaws in a computation are used to uncover secrets.

d) Acoustic investigation: attacks that take advantage of sound generated by a computation (similar to power analysis).

2.2 Advance Encryption Standard Algoritm

Advance Encryption Standard Rijndael Algorithm Designed by Vincent Rijmen and Joan Daemen .

2.2.1 Attack by AES:

XSL Attack method has a high work factor, which means that it does not reduce the effort required to break AES in comparison to an exhaustive search unless it is reduced. Therefore, it will have no immediate effect on block ciphers' actual security. Nevertheless, the attack has prompted experts to be more concerned about the current AES's algebraic simplicity.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1979 – 1988

In general, the XSL attack is based on deriving a system of quadratic simultaneous equations by first examining a cipher's internals. Most of the time, these systems of equations are very big, like the 128-bit AES, which has 8000 equations and 1600 variables. These systems can be solved in a number of ways. The specialized algorithm known as XSL (eXtended Sparse Linearization) is then utilized in the XSL attack to solve these equations and retrieve the key.

The attack stands out because it only requires a small number of known plaintexts to be executed; Linear and differential cryptanalysis, for example, required a disproportionately large number of known or selected plaintexts in the past.

2.2.2 The Encryption key and its Expansion

Assuming a 128-bit key, the key is also set up as a 4 by 4 byte array. The first word from the key occupies the first column of the matrix, just like with the input block, and so on.

A table of 44 words is created from the four column words of the key matrix.[2]

Four words from the key plan are consumed for each round. 4-byte words used as the encryption key, which is then expanded into a key plan made up of 44 4-byte words.

2.2.3 The Overall Structure of AES

Fig. 2 depicts the Structure of AES encryption and decryption. When the encryption key is 128 bits long, the amount of rounds is 10.

Number of rounds is 12 when the key is 192 bits, and 14 when the key is 256.)

• The first four words of the key schedule are XORed into the input state array before any round-based encryption processing can begin. Decryption proceeds in the same manner, with the exception that we now XOR the ciphertext state array with the final four words of the key schedule.

• For encryption, there are four steps in each round:

1) Add a round key, 2) shift rows, 3) mix columns, and 4) substitute bytes.

The final step involves XORing four words from the key schedule with the output of the previous three steps.

- Each round of decryption consists of the following four steps:

1) Inverse mix columns, 2) Inverse change bytes,

3) Add a round key, and 4) Inverse shift rows

The output of the previous two steps is XORed with four words from the key schedule in the third step.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1979 – 1988

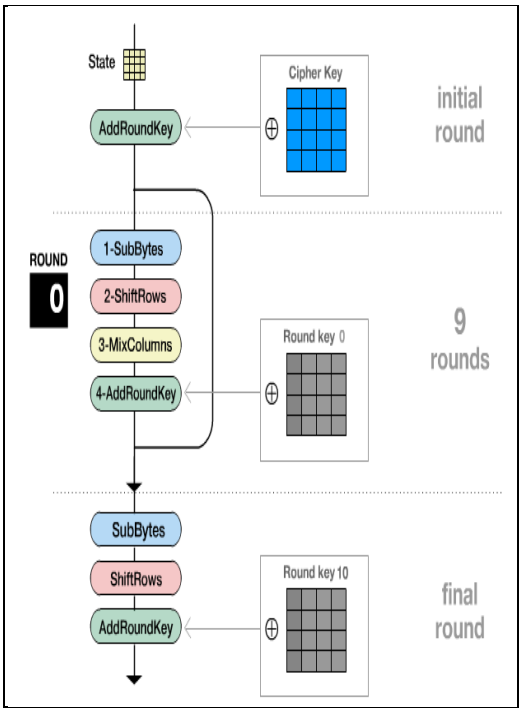

Fig.2 Structure of AES

Take note of the differences in the order in which shifting and substitution operations are carried out in an encryption round and in a decryption round, respectively.[4][5].

• The "Mix columns" step is not used in the final encryption round. The "Inverse mix columns" step is not used in the final decryption round.10

2.2 RSA Algorithm:

A popular public-key cryptosystem for secure data transfer is the RSA algorithm. It bears the names of Ron Rivest, Adi Shamir, and Leonard Adleman, who were its creators. The RSA algorithm belongs to the class of public-key implementations based on cryptography. The RSA calculation is in light of the numerical same, which is created by the English mathematician Clifford Cocks. In this equivalent, the large integers are factored and then returned in reverse order to their initial values. This is called prime factorization of the chose indivisible numbers. [3] The RSA algorithm is based on the idea that data is encrypted using an equation. The result of this equation is a number that is used in the reverse process. The public key and private key are two numbers that are known in the RSA. Because it would have no effect on the security of the encrypted data, the public key can be distributed to anyone. In the event of a loss, the private key poses the greatest risk of data compromise.

Key creation: In RSA, key creation comes first. RSA encrypts data using a secret key, and decrypts it using a public key.

a) Pick p and q, two prime integers.

b) Determine n = pq.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1979 – 1988
c) Determine phi(n)=(p-1)(q-1)

d) Select a number e such that gcd(e, phi(n)) = 1 e and 1 e phi(n) are true. Determine d so that d*e equals 1 mod phi.(n)

The secret key is made up of n and d, while the public key is made up of n and e.

Encryption: The sender must transform a message M into an integer m such that 0 = m n in order to encrypt it. Following that, the originator calculates the ciphertext c as follows:

c=me mod n

The recipient receives the ciphertext from the sender after that.

Decryption: The receiver calculates the plaintext m as follows in order to decode the ciphertext c:

M = C d n mod

2.3 Hybrid Algorithm:

By combining symmetric and asymmetric encryption algorithms is known as a hybrid cryptosystem [6] It combines the efficiency of symmetric encryption with the security of asymmetric encryption shown in Fig 3.

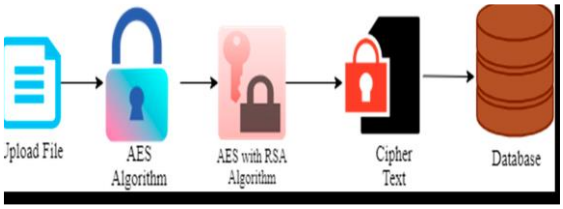

Fig 3. Hybird Encryption

Key Generation: The first step in a hybrid cryptosystem is key generation.

a) Generate a symmetric key K using a secure random number generator. b)Generate a public-private key pair using RSA.

Encryption: To encrypt a message M, the sender performs the following steps:

a) Generate a random initialization vector (IV) for symmetric encryption.

b) Encrypt the message M using a symmetric encryption algorithm such as AES, using the key K and IV. Let the resulting ciphertext be C.

c) Encrypt the key K using the receiver's public key, resulting in a ciphertext K'.

d) Transmit both C and K' to the receiver.

Decryption: To decrypt the message, the receiver performs the following steps:

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1979 – 1988
a) Decrypt the key K' using the receiver's private key, resulting in the key K.

b) Decrypt the ciphertext C using the key K and IV, resulting in the plaintext M.

Example:

Suppose Alice wants to send a message M to Bob using a hybrid cryptosystem.

Key Generation:

a) Alice generates a symmetric key K using a secure random number generator.

b) Alice generates a public-private key pair using RSA.

Encryption:

a) Alice generates a random initialization vector (IV) for symmetric encryption.

b) Alice encrypts the message M using a symmetric encryption algorithm such as AES, using the key K and IV. Let the resulting ciphertext be C.

c) Alice encrypts the key K using Bob's public key, resulting in a ciphertext K'. d) Alice transmits both C and K' to Bob.

Decryption:

a) Bob decrypts the key K' using his private key, resulting in the key K.

b) Bob decrypts the ciphertext C using the key K and IV, resulting in the plaintext M.

III.Comparative analysis

Evaluation Parameters: Each encryption method has strengths and weaknesses. We need to be familiar with the performance, strengths, and weaknesses of the various algorithms in order to select an appropriate cryptography algorithm for a given application. Consequently,[7][8][9] these calculations should be dissected in light of a few elements. The cryptosystems are analyzed in this paper using the following metrics, which can be used to compare them:

3.1 Encryption time

The time taken to change over plaintext to ciphertext is encryption time. The length of the encryption process is determined by the mode, the size of the plaintext block, and the size of the key. We measured encryption time in milliseconds for our experiment. The system's performance is affected by the encryption time. The system must be quick and responsive by reducing encryption time in Table 1 and Graphical representation in figure 4.

3.2 Decryption time

The time of recover plaintext from ciphertext is referred to as decryption time. In order to make the system responsive and quick, it is desired that the decryption time be less similar to

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1979 – 1988
the encryption time. The system's performance is impacted by decryption time. We measured decryption time in milliseconds during our experiment Table 2 and Graphical representation in figure 5.

3.3 Memory used

The amount of memory required for implementation varies depending on the encryption method. The algorithm's number of operations, key size, initialization vectors used, and type of operations all influence this memory requirement. The system's cost is influenced by the memory used. It is desirable to have the minimum amount of memory required.[10] Table 3 and Graphical representation in figure 6.

Graph Showing time required to get encryption and decryption processing time using different methods for 10 kb file,20kb and 30 kb files and Memeory used in MB.

Techniq ue used	**Average Response time for result processing(MS) in Project**		
Files	10kb files	20kb files	30kb files
AES	0.7	1.4	2.1
RSA	0.9	1.9	2.9
Hybrid	0.98	2.35	3.15

Table 1. Processng Time of encryption technique

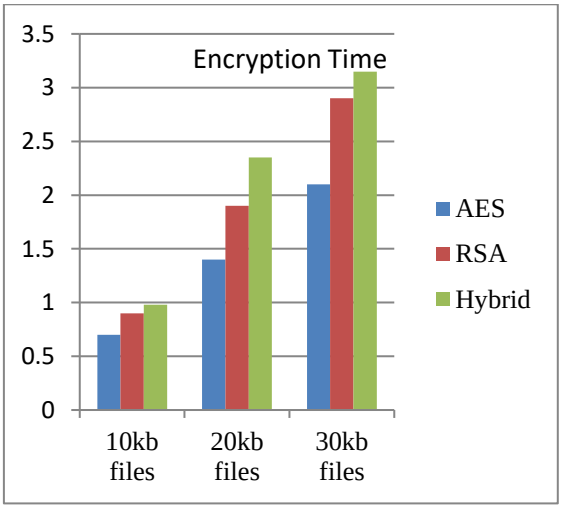

Fig 4. Graphical Representation of Processng Time of encryption technique

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1979 – 1988

Technique used	**Average Response time for result processing(MS) in Project**		
Files	10kb files	20kb files	30kb files
AES	0.5	1.2	1.9
RSA	0.8	1.5	2.7
Hybrid	0.89	2.15	3.1

Table 2. Processng Time of Decryption

In the above graph the x axis indicates the number of techniques applied in project. The y axis indicated the total computational time in ms (Milli Seconds) to perform encryption calculation.

In this above table execution time is calculated this can be calculated with the help of the one query.

i.e SET STATISTICS TIME ON

GO

Select computation matrix

GO

SET STATISTICS TIME Off

This execution time may vary it's depend on the system configuration.

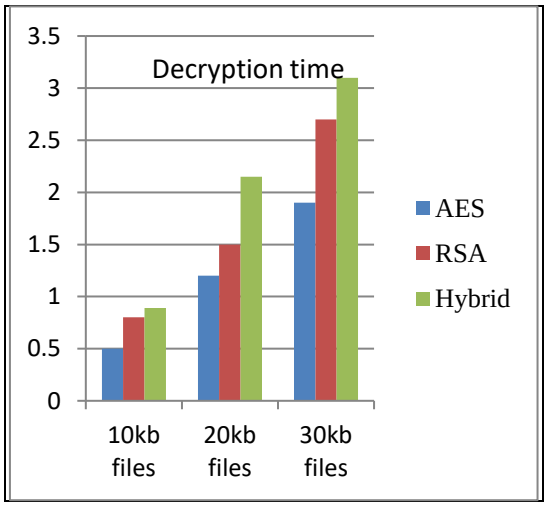

Fig 5. Graphical Representation of Processng Time of decryption technique

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1979 – 1988

Technique used	Average Memeory Used Size in MB
AES	15.1
RSA	31.5
HYBIRD (AES+RSA)	17.756

Table 3. Average Memory used in MB

The hybrid method ensures confidentiality when logging into the online system. This method uses various encryption methods to encrypt the password while providing the username in clear text. The user's legitimacy is then verified by comparing the identity and password to those that have already been saved

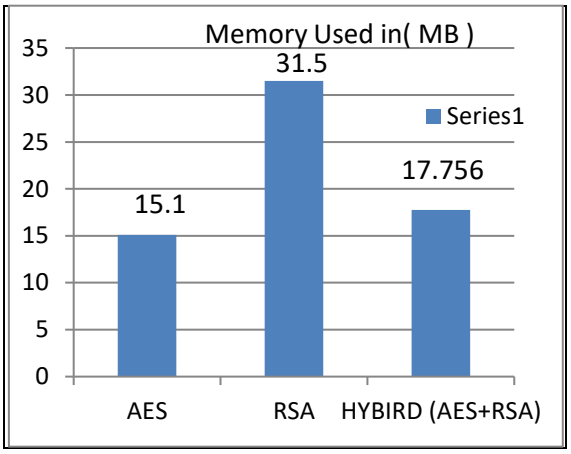

Fig 6. Graphical Representation for Average Memory used in MB

. The login and password that are saved in the cloud will be used to identify any user who has tempered with the data, which can speed up the process of determining the underlying cause of data tempering. The password is encrypted while the username is displayed in clear text. The RSA method is then used to re-encrypt the encrypted output..

The double encryption model, which encrypts the data twice before uploading it to the cloud, can speed up the process of determining the root cause of the problem. The AES algorithm is used to encrypt plain text and the RSA-1024 algorithm is used to encrypt the AES key. The operation of the double encryption scheme is depicted .The strength of this method is that RSA ensures high security while AES reduces the time complexity of file sharing.[11] Key management and the overhead of encryption and decryption for large files are this method's used.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1979 – 1988

IV. Conclusion

The strength of this approach is that it uses a hybrid approach by using RSA and AES encryption methods for providing data security. The use of RSA increases the difficulty level to hack the data, whereas AES reduces the time required to transfer files between the user and cloud data storage. The weakness is that encryption and decryption time is overhead for large file sizes. The proposed approach is that if the file size increases, the number of keys manage the storage space and by which utilization of memory size is minimize using hybrid method.

References

1. Ali Abdulridha Taha,"Enhancement the Security of Cloud Computing using Hybrid Cryptography Algorithms", International Journal of Advancements in Computing Technology · December 2017.
2. Dickson Kodzo Mawuli Hodowu, "An Enhancement of Data Security in Cloud Computing with an Implementation of a Two-Level Cryptographic Technique, using AES and ECC Algorithm", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181,Vol. 9 Issue 09, September-2020
3. Muhammad Bilal Qureshi, "Encryption Techniques for Smart Systems Data Security Offloaded to the Cloud" Symmetry 2022, 14, 695. https://doi.org/10.3390/sym14040695
4. S. N. Mendonca, "Data Security in Cloud using AES," International Journal of Engineering Research & Technology (IJERT), vol. 7, pp. 205-208, 2018.
5. Arvind K. Sharma, "Cryptography & Network Security Hash Function Applications, Attacks and Advances: A Review ", International Conference on Inventive Systems and Control (ICISC 2019) IEEE Xplore Part Number: CFP19J06-ART; ISBN: 978-1-5386-3950-4
6. De Rosal Ignatius Moses Setiadi , "A Comparative Study MD5 and SHA1 Algorithms to Encrypt REST API Authentication on Mobile based Application" , 2019 International Conference on Information and Communications Technology (ICOIACT).
7. Khan, S.S.; Tuteja, R.R. Data security in cloud computing using cryptographic algorithms. Int. J. Innov. Res. Comput. Commun.Eng. 2019, 7, 1.
8. Salama, D. Improving the security of cloud computing by building new hybrid cryptography algorithms. Int. J. Electron. Inf. Eng.2018, 8, 40–48.
9. Das, D. Secure cloud computing algorithm using homomorphic encryption and multi-party computation. In Proceedings of the International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 10–12 January 2018; pp. 391–396.
10. Akhil K.M, "Enhanced Cloud Data Security Using AES Algorithm", 2017 International Conference on Intelligent Computing and Control (I2C2).
11. M. Thangapandiyan, "Enhanced Cloud Security Implementation using Modified ECC Algorithm", International Conference on Communication and Signal Processing, April 3-5, 2018, India.