International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 1
DOI: https://doi.org/10.17762/ijfrcsce.v8i1.2083
***Article Received**: 24 December 2021 **Revised**: 16 February 2022 **Accepted**: 22 February 2022 **Publication**: 31 March 2022*

Enhancement for Secured File Storage Using Modern Hybrid Cryptography

Oshin Dhiman
Information Technology Programmer Analyst,
LaSalle College, Montreal
oshin.dhiman@gmail.com

Dr. Anand Sharma
Asst. Prof., Department of CSE,
Mody University of Science and Technology, Lakshmangarh
https://orcid.org/0000-0002-9995-6226
anand_glee@yahoo.co.in

Abstract

In a wide range of applications, from cloud storage to chat messaging, security is a major issue. In today's business world, there are several security dangers as well as a fiercely competitive environment. Thus we want a secure file storage solution to safeguard and convey their confidential data. Cryptography is a technique for encrypting or decrypting data to store information secretly and conceal its true meaning. The existing techniques include the fact that heavily encrypted, valid, and digitally signed material might be hard to obtain, even for an authorized user, at a time when access is essential for making decisions. This research suggests a modern hybrid cryptographic method to strengthen the security of file storage. The proposed algorithm follows the flow mentioned here: data collection, normalization technique is used for data preprocessing, and Advanced Encryption Standard (AES) is used for data encryption. Combining symmetric and asymmetric algorithms contributed to the growth of the modern hybrid cryptography algorithm. There are two types of encryption algorithms: Data Encryption Standard (DES), which is symmetric, and Rivest, Shamir, & Adleman (RSA), which is asymmetric. These two types of algorithms are then compared to see how well they perform in terms of encryption/decryptions time, key generation time, & file size. The proposed algorithm is very effective in enhancement for secured file storage using modern hybrid cryptography.

Keywords: *Cryptography, Encryption, Decryption, Hybrid Cryptography Algorithm, Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivest, Shamir, and Adleman (RSA).*

I.INTRODUCTION

The art of cryptography involves transforming the actual data from the sender side into an unreadable format and translating the unreadable format from the receiver side back into the actual data. Algorithms are used to accomplish various aspects of cryptography. Symmetric and asymmetric cryptographic algorithms are both subclasses of the same algorithm. Symmetric key methods encrypt and decrypt data using the same secret key and thereby simplify the encryption process. Because encryption and decryption are performed secretly, these algorithms are also known as private key algorithms. There are two kinds of keys used in asymmetric algorithms: public and private. Asymmetries involve encryption and decryption via a public key, (Lalithambikai & Vanitha (2018)). Data encryption and decryption is a key components of cryptography as a means of securing data privacy, secrecy, & integrity. In cryptography, the four primary objectives are data secrecy, integrity, authentication, and non-repudiation. Cryptography methods include encryption, hashing algorithms, messages authentication code (MAC), and digital signatures, (Akomolafe and Abodunrin (2018)).

Hybrid encryption is considered exceptionally safe as long as the public & private key are kept secret. Symmetric and hybrid cryptographic is utilized to transmit data over a network. Public key encryption protects random symmetric key encodings. The recipient then uses a public key encryption method to decrypt the symmetric key. Decryption begins after the symmetric key has been recovered, (Patil and Bansode (2020)). Building secure systems to guard against data breaches necessitates the use of cryptographic algorithms. The Data Encryption Standards (DES) is a well-known cryptographic method that has been widely used in numerous security products. However, due to the significant success of cryptanalysis attacks and the comparatively low keyword length at only 56 bits, serious concerns have been raised about long-term security, (Saravanan and Kalpana (2018)). Figure 1 shows the representation of general hybrid cryptography.

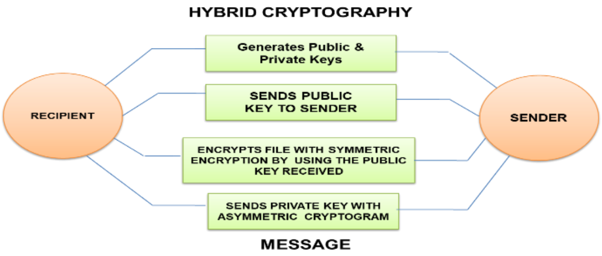

HYBRID CRYPTOGRAPHY
Generates Public & Private Keys
SENDS PUBLIC KEY TO SENDER
ENCRYPTS FILE WITH SYMMETRIC ENCRYPTION BY USING THE PUBLIC KEY RECEIVED
SENDS PRIVATE KEY WITH ASYMMETRIC CRYPTOGRAM
RECIPIENT
SENDER
MESSAGE

Figure 1. Hybrid cryptography

Encryption is the process of encrypting data so that only those who have the proper credentials may access it. As a means of protecting information, it is quite effective. Most cryptographic methods have the following elements: plain text, ciphertext, key, and algorithm. The primary goal of a cryptographic mechanism is to protect sensitive data from unwanted access. Encryption and decryption are the two most important cryptographic operations, (Acholli and Ningappa (2019)). There are various drawbacks to using a hybrid cryptography protocol in key distribution methods, according to this research. The flaws and risks that arise from poorly designed systems, protocols, & procedures are not protected by cryptography. Defensive infrastructure must be properly designed and set up to address these issues.

Hence in this paper, the enhancement for secured file storage using modern hybrid cryptography was described. The further part of this article is categorized as follows: Part II provides the related works and problem statement; Part III explains the proposed method; Part IV explains the performance analyses; Part V explains the conclusion.

II. RELATED WORKS

(Soni and Malik (2022)) described various hybrid cryptography models in general terms, enhancing data security. In addition, various standard and hybrid approaches for data security are examined side by side in the article. If exceptional security is desired, the hybrid approach should be used instead of AES. Models that integrate public-key RSA cryptography with the exchange of Diffie Hellman (DH) keys to mitigate man-in-the-middle (MITM) attacks have been proposed, (Gupta and Reddy (2022)). Based on comparisons with other cryptographic systems like DH Key Exchanges and the RSA Cryptosystem, this model's efficacy was determined. Monitoring industrial operations over the internet can be made safer and more efficient with this new security algorithm. DES, RC4, and AES are among the algorithms proposed by (Bharali et al. (2020)), which would encrypt data using a combination of these and other well-known methods. The algorithm's key and the information about the encrypted portion of the file will be included in the key information. (Chaudhari et al. (2018)) presented an overview of the data security issue. Data can only be deciphered by someone who knows how to decode it back to its original form using cryptography techniques. Today's computer systems rely heavily on cryptography to ensure that sensitive information is protected and to ensure that it is authenticated. (Nithya et al. (2022)) examined various network security concerns, the role of cryptography in securing networks, and the encryption and decryption processes using various types of cryptography. It also describes the different types of key algorithms which have been used for network security purposes in this work. The symmetric and asymmetric general structures are given below.

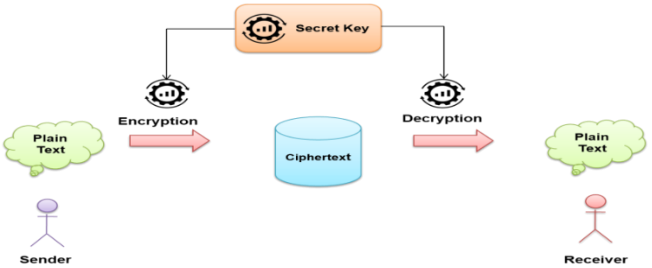


Figure 2. General Structure of Symmetric Key Algorithm

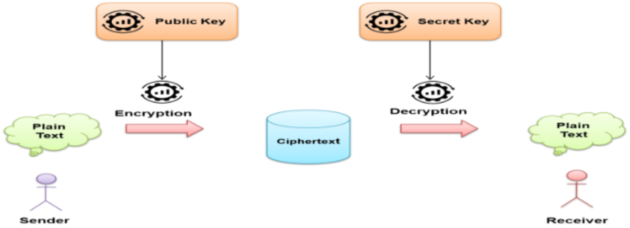


Figure 3. General Structure of Asymmetric Key Algorithm

(Rakheja et al. (2019)) presented a hybrid cryptosystem with superposition of coherence, modulus equals & breakdown by chance. To further enhance the cryptosystem's security, pixel swapping is performed via a hyperchaotic system. (Noor et al. (2022)) explained the underlying differences between the various types of cryptography and provides examples of how they can be used to encrypt data. (Pooja and Chauhan (2022)) presented a new symmetric and asymmetric cryptography technologies are combined in this new method. Since symmetric methods provide high levels

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 1
DOI: https://doi.org/10.17762/ijfrcsce.v8i1.2083
***Article Received**: 24 December 2021 **Revised**: 16 February 2022 **Accepted**: 22 February 2022 **Publication**: 31 March 2022*

of security, while asymmetry approaches facilitate key management, the proposed algorithm incorporates AES, DES, and a modified Rivest–Shamir–Adleman (m-RSA) algorithm. (Basapur and Shylaja (2021)) stated that several vulnerabilities to the confidentiality of information can be identified by using a hybrid cryptographic approach that combines AES with RSA. Using masking and hybrid cryptography, it is possible to send large amounts of data securely over the cloud.

Problem statement

There are a variety of dangers to the data that customers store on the networks of service providers. Data integrity refers to the degree of trust in the network that the data it contains is exactly what it should be and that it is safe from unauthorized alteration, whether accidental or purposeful. As a result, a network service user can no longer completely rely on the network service provider to assure the storage of his critical data. It's also possible for data to leak out of the system due to criminal hacks of network providers or user account compromises. Instead of relying on the network service provider, use file encryption & stronger passwords.

III. PROPOSED METHODOLOGY

This part outlines the proposed procedure's overall flow. The schematic representations of a suggested technique includes the processes like data collection, data preprocessing using normalization, data encryption using advanced encryption standards, modern hybrid cryptography using data encryption standards, and rivest shamir and adleman algorithm, and data decryption.

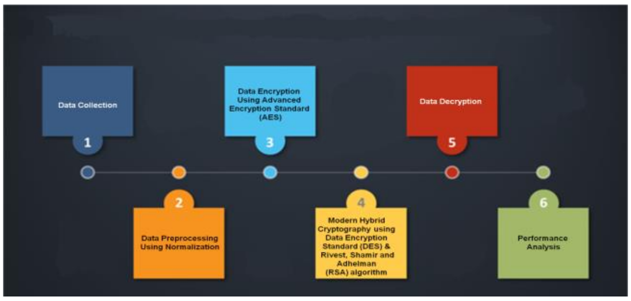

Data Collection
1
Data Encryption Using Advanced Encryption Standard (AES)
3
Data Decryption
5
2
Data Preprocessing Using Normalization
4
Modern Hybrid Cryptography using Data Encryption Standard (DES) & Rivest, Shamir and Adhelman (RSA) algorithm
6
Performance Analysis

Figure 4: Flow of proposed work

A) Data collection

An "EPM" (Educational Process Mining) has been discovered in a UCI machine learning repository. Learning analytics can benefit from access to data. Each of the six study sessions yielded a different time series of student activity. Students' information is stored in six folders for each session. There are 230318 instances and 13 attributes in the collection, all of which have integer characteristics. Table 1 lists the attributes of the dataset, (Chilambarasan and Kangaiammal (2021)).

Table 1. Description of an attribute

S.no	Features	Description
1.	Sessions	1 to 6 lab sessions will be held.
2.	Students-ID	ID number for 115 students (1, 2, 3....115).
3.	Exercise	It demonstrates the Ex. works. The student's ID number. (Es 2 1 stands for Exercise 1 from Session 2).
4.	Activity	There are 15 subcategories of physical activity. Making Use of Finite State Machine Simulators, the Deeds Simulator, a Text Editor, the Diagram, and Other Irrelevant Activities.
5.	Start-time	Date and time when a particular activity will begin.
6.	End-time	Date and time that activity ends.
7.	Idle-time	An amount for downtime among the beginning & end times.
8.	Mouse-wheel	volumes for mouse wheel movements made throughout a task.
9.	Mouse-wheel click	Numbers for mouse wheel clicks made while performing an action.
10.	Mouse-click-left	Count for left mouse clicks made during a specific activity
11.	Mouse-click right	An activity's numbers of right mouse clicks.
12.	Mouse movement	The mouse's distance travelled during an activity.
13.	Keystroke	Keyboard actions performed in a given period of time.

B) Data preprocessing using normalization

Dataset normalization can be accomplished using a variety of techniques, such as Min-Max normalizing, z-score normalization, decimal scaling, standardized moment, etc. The two common and extensively utilized normalization techniques are min-max and z-score normalization. Min Max technique was used for our work.

Min-Max normalization

The following equation is used in min-max normalization to normalize features in the range [0,1].

$$u' = \frac{u - min_B}{max_B - min_B} \qquad (1)$$

The minimum and maximum values of feature B are shown here by min_B and max_B, respectively. The values u and u' indicate the attribute's original and normalized values, respectively. The maximum and minimum feature values are transferred to 1 and 0, respectively, as can be seen from the equation above.

C) Data encryption using advanced encryption standards

129-bit blocks are used in AES' encryption, which makes it a block cypher. AES-129, AES193, and AES-257 are the three variations of AES based on the length of the key. 4 words, each of 32 bits, make up an AES 128-bit block. The AES algorithm begins by writing a 128-bit data block consisting of four words into the state sequence, and this sequence is used to complete all of the method's necessary actions. Having completed the final operation necessary to perform encryption, the output sequence's last state is written to it.

The first block of the AES algorithm is called the round conversion block, while the second block is called the key creation block. Repetitive structure, 129, 193, and 257-bit, depending on a key length, is repeated 11, 13, and 15 times in turn in the algorithm's repetitive structure. Table 2 lists the number of repetitions.

Table 2. Comparing AES Key block rounds

	Dimensions of a block (bit)	Length of the Key (bit)	Number of Rounds (Nr)
AES-129	129	129	11
AES-193	129	193	13
AES-257	129	257	15

Figure 5 shows how the status sequence is updated with the encrypted block at a beginning of the process. Once the input key and state sequence are added, encryption begins. Depending on length of the key sizes, the conversions are performed 10, 12, and 14 times.

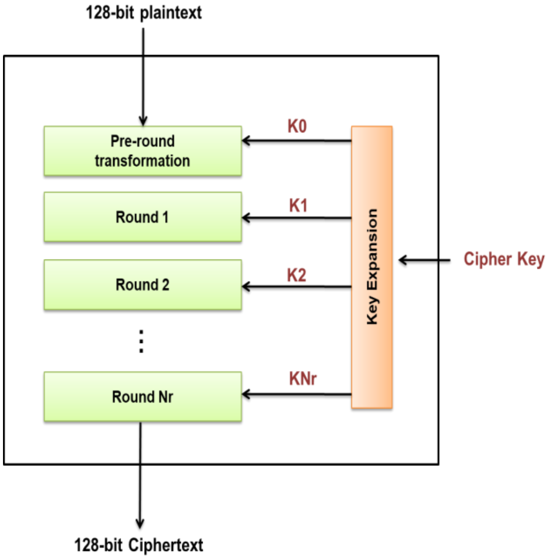


Figure 5. The AES Encryption's Structure

D) Modern hybrid cryptography using data encryptions standard and rivest Shamir and adleman algorithm

One of the most popular block ciphers is the Data Encryption Standards (DES). The sender's 64-bit plaintext is converted into the receiver's cipher text using the DES encryption process, which is unique. Encryption and decryption of data with DES need only 54 bits of the key. There are 16 rounds for Feistel structures used to encrypt the data in the DES encryption. According to a DES algorithm, a cipher generates a unique 48-bit key which is generated in figure 6.

A 64-bit block of data is first permuted using a 64-bit permutation. A 32-bit subblock, L0, is created, and this is transmitted to Feistel rounds. This will continue until the encryption method has gone through a total of 16 rounds. The higher the number of rounds, the higher the level of security. Pre-output is generated in the 16th round by swapping out L15 and R15. Finally, an inverse function of a initial permutation can be obtained by combining [R15, L15].

***Article Received**: 24 December 2021 **Revised**: 16 February 2022 **Accepted**: 22 February 2022 **Publication**: 31 March 2022*

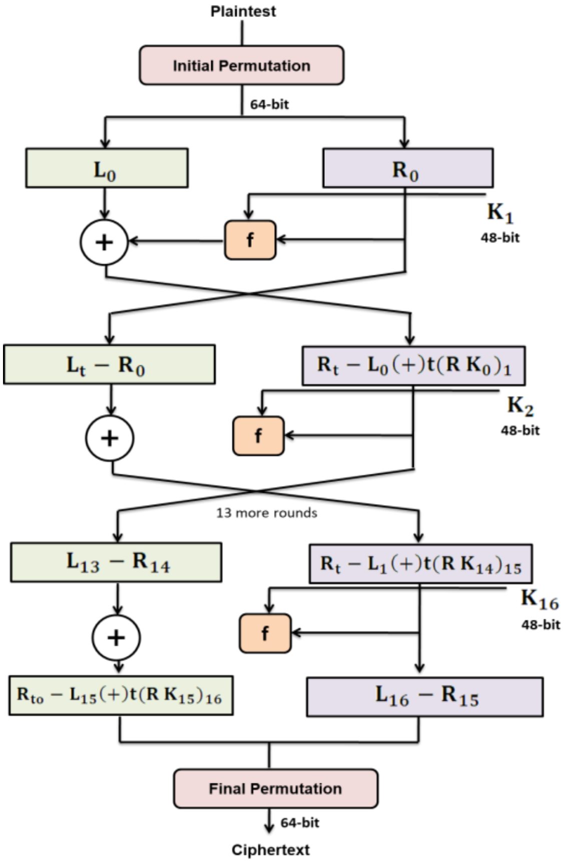
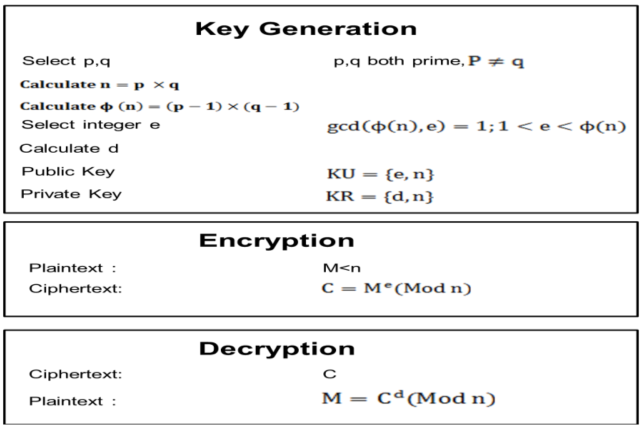


Figure 6. Encryption with DES

The public key and a private key are used in RSA, an asymmetric algorithm. Everyone can see the public key, but the private key is kept secret. The RSA algorithm is named after its creators, Rivest, Shamir, and Adleman. People know RSA for its secure way of encrypting data. RSA is based on prime numbers that are positive integers and are used exponentially to encrypt and decrypt data. The steps of the RSA algorithm are shown in figure 7.



Key Generation

Select p,q	p,q both prime, $P \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1) \times (q-1)$	
Select integer e	$gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	
Public Key	$KU = \{e, n\}$
Private Key	$KR = \{d, n\}$

Encryption

Plaintext :	M<n
Ciphertext:	$C = M^e(\mathrm{Mod}\ n)$

Decryption

Ciphertext:	C
Plaintext :	$M = C^d(\mathrm{Mod}\ n)$

Figure 7. RSA algorithm

There were two exponent variables in this algorithm: e stands for "public" & d stands for "private." "Plaintext" and "cipher text" are used to explain the encryption & decryption process, respectively.

Encryption: $C = M^e \ mod \ n$ (2)

Decryption: $M = C^d \ mod \ n$ (3)

Where n is a large number that is used for generating keys. When it comes to secure data storage & communication, there are various drawbacks to employing the DES and RSA algorithms combined. Improved encryption and decryption methods have been provided in this research to improve the current model's security.

E) Data decryption

Decryption refers to the process of recovering encrypted data and re-encoding it in its original format. As a general rule, it is a decryption procedure in reverse. The secret key or password is required to decrypt the encrypted data, so it can only be decrypted by an authorized user. Data security is an important consideration when putting in place an encryption and decryption system. Keeping tabs on unwanted access to information on the Internet is an essential precaution. Because of this, data is encrypted so that it cannot be stolen or lost. Text files, photos, e-mails, user data, and directories are just a few of the things that are commonly encrypted. To access encrypted data, the recipient for decryption is presented with a popup or window that asks for a password to be provided. Extracting and converting jumbled data into words & images which can be understood by both a reader and a system is the first step in decryption. Automated or manual, decryption is possible. It can also be done with a password or a set of keys.

IV. RESULTS AND DISCUSSION

The overall behavior of the recommended framework is discussed in this section. Figures 8, 9, 10, and 11 show the comparison of parameters, like security level, encryption time, decryption time, and execution time for existing and proposed methods. For example, among the approaches that may be utilized are the advanced encryption standard (AES), blowfish (BF), elliptic curve integrated encryption scheme (ECIES), and data encryption standard with rivest, shamir, and adleman (DES+RSA).

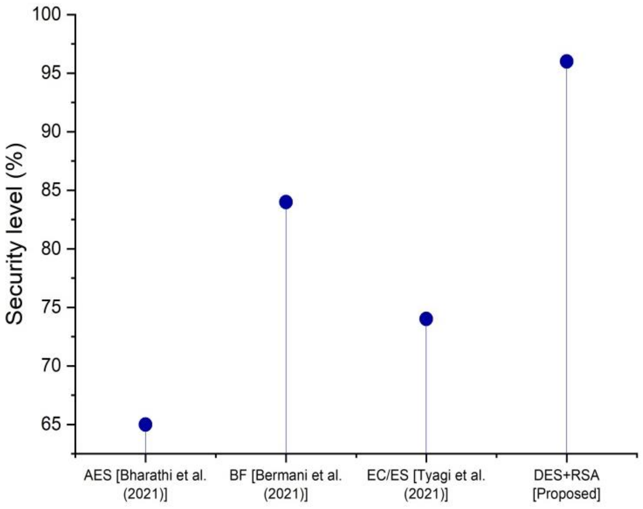


Figure 8. Security level results of proposed and existing methodology

Figure 8 represents the security level results with proposed and existing approaches. The above figure 8 shows that the proposed method of data encryption standard with rivest, shamir, and adleman has a high-security level when compared to the existing methods such as advanced encryption standard, blowfish, elliptic curve integrated encryption scheme.

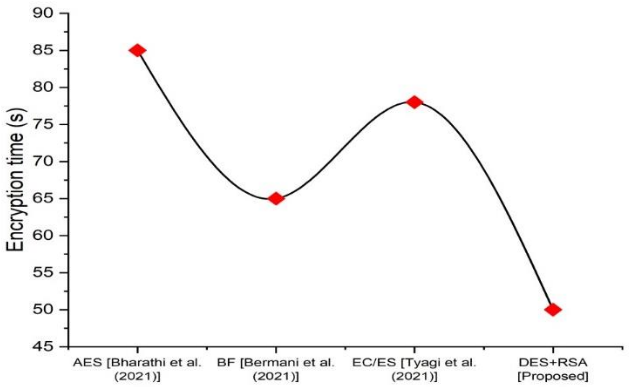


Figure 9. Encryption time results of proposed and existing methodology

Figure 9 represents the encryption time results with proposed and existing approaches. The above figure 9 shows that the proposed method of data encryption standard with rivest, shamir, and adleman has low encryption time when compared to the existing methods such as advanced encryption standard, blowfish, elliptic curve integrated encryption scheme.

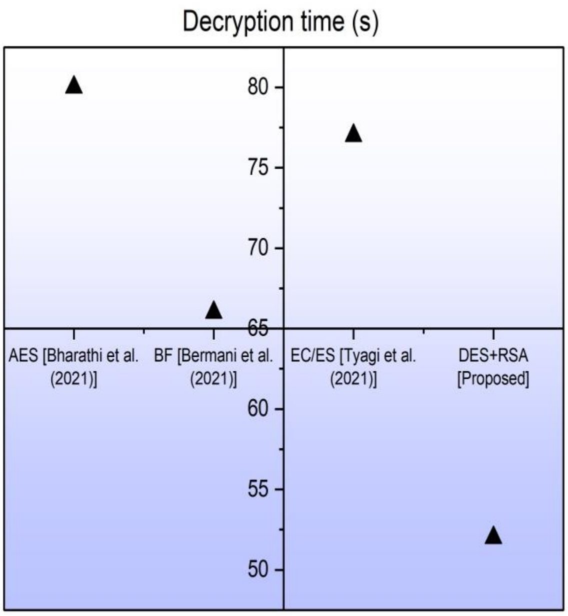


Figure 10. Decryption time results of proposed and existing methodology

Figure 10 represents the decryption time results with proposed and existing approaches. The above figure 10 shows that the existing methods such as advanced encryption standard, blowfish, and elliptic curve integrated encryption scheme has high decryption time when compared to the proposed method of data encryption standard with rivest, shamir, and adleman.

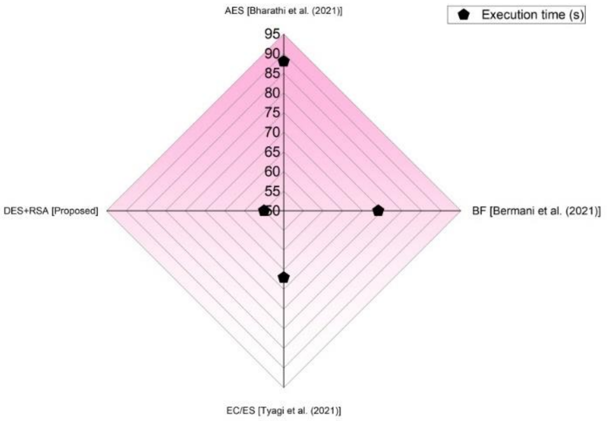


Figure 11. Execution time results of proposed and existing methodology

Figure 11 represents the execution time results with proposed and existing approaches. Figure 11 shows that the proposed method of data encryption standard with rivest, shamir, and adleman has a low execution time when compared to the existing methods such as advanced encryption standard, blowfish, elliptic curve integrated encryption scheme.

V. CONCLUSION

The term "hybrid cryptography" refers to a technique that combines symmetric and asymmetric encryption techniques. To achieve the highest level of security, a hybrid cryptosystem integrates symmetric and asymmetric cryptography. This project implements a data encryption standard with rivest, shamir, and adleman. As symmetric & asymmetric key cryptographic methods are employed in the encryption of the file, it is safe. The hybrid encryption system is far safer and more robust than a simple encryption system. Moreover, the performances like security level, decryption time, encryption time, and execution time are examined and matched with the existing approaches and proposed method.

REFERENCES

[1]. Lalithambikai, A. and Vanitha, M., 2018. An Efficient Technique for Cryptography with Enhanced Key Security. *International Journal of Pure and Applied Mathematics*, *118*(8), pp.479-484.

[2]. Akomolafe, O.P. and Abodunrin, M.O., 2018. A hybrid cryptographic model for data storage in mobile cloud computing. *International Journal of Computer Network and Information Security*, *9*(6), p.53.

[3]. Patil, P. and Bansode, R., 2020. Performance evaluation of hybrid cryptography algorithm for secure sharing of text & images. *International Research Journal of Engineering and Technology*, *7*(9), pp.3773-3778.

[4]. Saravanan, P. and Kalpana, P., 2018. The novel reversible design of advanced encryption standard cryptographic algorithm for wireless sensor networks. *Wireless Personal Communications*, *100*(4), pp.1427-1458.

[5]. Acholli, S. and Ningappa, K.G., 2019. VLSI implementation of hybrid cryptography algorithm using LFSR key. *International Journal of Intelligent Engineering and Systems*, *12*, pp.10-19.

[6]. Soni, P. and Malik, R., 2022. A Comparative Study of Various Traditional and Hybrid Cryptography Algorithm Models for Data Security. In *Modeling, Simulation and Optimization* (pp. 31-47). Springer, Singapore.

[7]. Gupta, C. and Reddy, N.S., 2022. Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography. In *Journal of Physics: Conference Series* (Vol. 2161, No. 1, p. 012014). IOP Publishing.

[8]. Bharali, D., Medhi, D., Singh, W.S., Haque, A., and Nath, K., 2020. Secure Files Storage in Cloud using Hybrid Cryptography. *i-manager's Journal on Cloud Computing*, *7*(2), p.8.

[9]. Chaudhari, S., Pahade, M., Bhat, S., Jadhav, C., and Sawant, T., 2018. A research paper on a new hybrid cryptography algorithm. *International Journal for Research and Development in Technology*, *9*(5), pp.1-4.

[10]. Nithya, B., Mathew, J.C., Kavya, G., Anutha, N.R. and Kumari, A., 2022, February. An Analysis on Cryptographic Algorithms for Handling Network Security Threats. In *2022 IEEE Delhi Section Conference (DELCON)* (pp. 1-9). IEEE.

[11]. Rakheja, P., Vig, R. and Singh, P., 2019. An asymmetric hybrid cryptosystem using equal modulus and random decomposition in hybrid transform domain. *Optical and Quantum Electronics*, *51*(2), pp.1-26.

[12]. Noor, S.E., Ahmad, A., Martos Núñez, M.V. and Hornos Barranco, M.J., 2022. Learning the basics of cryptography with practical examples.

[13]. Pooja and Chauhan, R.K., 2022. Triple phase hybrid cryptography technique in a wireless sensor network. *International Journal of Computers and Applications*, *44*(2), pp.148-153.

[14]. Basapur, S.B. and Shylaja, B.S., 2021. A Hybrid Cryptographic Model Using AES and RSA for Sensitive Data Privacy Preserving. *Technology*.

[15]. Chilambarasan, N.R. and Kangaiammal, A., 2021. Reinforced Streebog Cryptographic Hash Blockchain Based Access Control for E-Learning in Cloud. *Advances in Dynamical Systems and Applications*, *16*(2), pp.1349-1370.

[16]. Bharathi, P., Annam, G., Kandi, J.B., Duggana, V.K. and Anjali, T., 2021, July. Secure file storage using hybrid cryptography. In *2021 6th International Conference on Communication and Electronics Systems (ICCES)* (pp. 1-6). IEEE.

[17]. Bermani, A.K., Murshedi, T.A. and Abod, Z.A., 2021. A hybrid cryptography technique for data storage on cloud computing. *Journal of Discrete Mathematical Sciences and Cryptography*, *24*(6), pp.1613-1624.

[18]. Tyagi, M., Manoria, M. and Mishra, B., 2021. Implementation of cryptographic approachesin proposed secure framework in cloud environment. In *Intelligent Computing and Applications* (pp. 419-426). Springer, Singapore.