International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/209990 Volume 8, Issue 5, September – October (2021)

RESEARCH ARTICLE

Efficient Cipher Scheme for Hybrid Models with Internal Structure Modification

Pravin Soni
Department of Computer Science and Engineering, Lovely Professional University, Punjab, India
pravindsoni@gmail.com

Rahul Malik
Department of Computer Science and Engineering, Lovely Professional University, Punjab, India
malikvnit@gmail.com

Received: 21 August 2021 / Revised: 18 September 2021 / Accepted: 23 September 2021 / Published: 27 October 2021

Abstract – Data confidentiality (DC) became an essential security service required during data transmission or storing sensitive data over the network in every application. A rise in security attacks causing several security services are required to be implemented for preventing both passive and active attacks. DC security service is most common and based on a complex reversible mathematical calculation recognized as cipher algorithm. The confidentiality of information kept in digital mode, as well as its simple accessing at any moment, has become a significant phenomenon. However, many applications put constrained to develop cipher models that can provide better performance while maintaining minimum security level. In this regard, several hybrid models have been developed and discussed in the literature based on cascading which provides enhanced security but increases system performance due to the running of multiple algorithms. The aim of the proposed scheme is to improve the system performance of the cascaded hybrid model by doing modifications in the internal structure of each algorithm used in the model by reducing the number of rounds required for doing encryption and decryption. Each algorithm used in cascading in hybrid model uses a different key generated using the SHA256 algorithm which helps to maintain the security level of the hybrid cryptography model. Finally, we conduct the performance analysis of the existing hybrid cryptography model with the proposed cipher scheme having a reduced number of rounds. The proposed scheme shows better performance of the hybrid model compared with its corresponding existing model.

Index Terms – Data Confidentiality, Hybrid Cryptography, Internal Modification, Cascaded Encryptions, Secure Hash Algorithm.

1. INTRODUCTION

With the widespread and rapid developments of internet-based applications, the security of personal and private information requires the highest priority of attention for daily routine life. Preventing and controlling unauthorized access to private and personal information is always considered as the utmost issue by application developers and users of applications [1]. This issue has been resolved by utilizing the concept of cryptography. Cryptography (the technique of using coded messages) is used as a way of transforming data into a scribbled form. There is a need for cryptography for securing personal and private information from unauthorized access [2], [3]. Cryptography offers various services to be utilized by application developers for performing user authentication, data validation, data confidentiality, etc. Numerous encryption algorithms are available, which proved efficient for providing DC services [1]. Symmetric algorithms are considered the most efficient and cost-effective algorithm for data confidentiality. Moreover, the DC security service is typically based on a strong symmetric cipher algorithm [2].

The encryption algorithm is mainly categorized into two types based upon key utilization: conventional (symmetric) or public-key (asymmetric) algorithm. Symmetric encryption algorithm also known as conventional algorithm utilizes a single secret key for encryption and decryption process. AES (Rijndael), DES, Blowfish, IDEA, RC-6, Twofish, MARS, Serpent are some popular used symmetric algorithms. Asymmetric encryption algorithm (public-key encryption algorithm) requires two keys, one for encryption and the other for decryption. RSA, EC are some popular asymmetric algorithm [3].

Cryptographic algorithm modifications can be categorized mainly into two broad categories as “internal” and “external” modification. Internal modification means changing the basic internal structural unit of the algorithm, to increase its throughput and complexity. The internal modification may offer great cryptographic strength, but it needs a huge experience to preserve the basic concept of the initial security algorithm. Apart from this, the time and cost required can be extremely high for internal modification of the algorithm and its implementation in hardware/software [4]. Internal modification could be increasing the size of the key required in the algorithm or adding the extra key i.e secondary key.

Many symmetric block ciphers have a Feistel structure which consists of a round performed several times. Each round performs substitution and permutation-based upon a secret key. The Internal modification in a symmetric block cipher could be simply changing of its S-boxes or modifying the number of rounds in the Feistel structure [4], [5]. D'souza and Panchal modified the internal structure of the AES algorithm by transforming static s-box to dynamic s-box and utilizing dynamic key generation process. The dynamic key is generated at random when the sender login in the system based on the current time and Dynamic S-box are created by transforming static substitute-box using cipher key which mainly involves XOR operation [6].

External modification means an amalgamation of two or more block algorithms to get new algorithms. The resultant algorithm is a “hybrid” algorithm, which includes multiple original algorithms as its core. The external modification is an easy and convenient method for the designer who doesn’t have much experience in cryptographic algorithm design. Furthermore, it offers more significant design flexibility and reduces time and cost for its implementation in hardware/ software [4], [7].

Hybrid cryptography can further enhance the DC security service to many communication systems which utilize multiple ciphers of the same or different types together by including the benefits of each cipher. Figure 1 illustrates how the several ciphers can be cascaded for enhancing the DC security service [2].

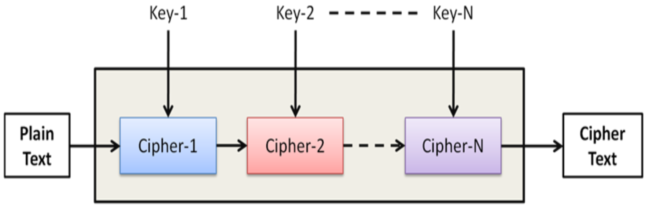

Figure 1 Hybrid Cascaded Encryption Model (n-tier) [2]

However, the existing hybrid cryptography solutions may not be suitable due to performance issues. The new emerging applications require faster processing time for a better user-friendly experience. Relying on hybrid cryptography, in this case, may lead to overhead on computational resources, such as the case with Super-Encryption [8] (IDEA and WAKE), which requires full encryption process of both algorithms in sequence, resulting in increased performance of the system. Hence there is a need for a new hybrid cryptography algorithm with high performance and enhanced security. The chaotic cryptography algorithm is not a good alternative due to proven insecure in numeral cases [9] and also requires floating calculations which complicates hardware implementation [10].

Based on the reviewed literature, it has been observed that many hybrid models lack system performance due to multiple encryptions. Hybrid models need a way to improve their performance to be utilized in today’s commonly used applications like cloud, chatting, etc for a better user experience. In particular, the proposed system tries to improve the performance of the hybrid model by modifying the number of rounds utilized in its Feistel structure. For this, various hybrid models are examined, and famous existing models are implemented for comparing the results.

2. LITERATURE REVIEW

This section entails a short overview of work accomplished in the field of hybrid cryptography algorithms for information security by numerous researchers. Abdullah *et al*, 2018 [8] developed a hybrid cryptography model using powerful IDEA and WAKE modern symmetric algorithm. The system first encrypts the plain text with IDEA and then re-encrypts using the WAKE algorithm which changes the data into hexadecimal format before encryption. Rachmawati et al., 2018 [11] developed a hybrid model which uses the IDEA algorithm for encrypting text messages and the knapsack algorithm for securely distributing the secret key used by IDEA for encryption. Tayel et al., 2018 [12] proposed a hybrid cryptosystem for protecting multimedia where image encryption is performed using SERPENT algorithm and key generation and sharing is managed using ECC algorithm. Timilsina & Gautam, 2019 [13] combined Blowfish and ECC to develop a hybrid cryptosystem. They prepared various hybrid models of this combination by varying the key size of the Blowfish algorithm and analyze the performance of various hybrid models.

Venkatraman & Geetha, 2019 [14] developed an enhanced hybrid model for a public cloud environment that uses the Blowfish algorithm and genetic operators. The model encrypts images multiple times, first by the Blowfish algorithm and then by genetic operators in a fixed sequence. The model outperforms the most commonly used algorithm in the cloud environment for image encryption. This proposed system will take more time than blowfish algorithm due to addition of extra layer of encryption with genetic operator.

Abroshan, 2021 [15] has designed a hybrid encryption model using Blowfish and ECC algorithm for cloud computing. Their model encrypts cloud data using the Blowfish algorithm and the key used in data encryption is encrypted using the ECC algorithm. The proposed model performance is satisfactory for small-size data but lacks for big-size data files.

Hussam *et al*, 2021 [16] have designed a hybrid model using PRESENT, TWINE, and 5-D Chaos Keys which performs 24 rounds for encrypting data. They have divided 128-bit data blocks into 2 parts for encryption with PRESENT and modified TWINE algorithms.

Mahmud *et al*, 2018 [17] have developed a hybrid model by cascading two famous encryption algorithms as AES and Blowfish. They have proposed this system for providing security to patient medical reports available in form of pdf file. They have observed that their model performance was better than the AES algorithm but less than the Blowfish algorithm.

Kaushik and Patel, 2019 [18] have developed a hybrid model AES-Twofish for cloud data security. They have concluded that their hybrid model performance in terms of encryption-decryption time is better than the AES-Blowfish hybrid model. Similar results were also observed and recorded by Neha, 2019[19].

Othman, 2017 [20] have developed a hybrid model for robot communication which involves securing small-sized commands by encrypting commands using RSA, Twofish, and AES in sequence. They concluded that this hybrid model requires more time to break using brute force attacks rather than these algorithms.

Rajan and James, 2013 [21] designed a hybrid model for text files by cascading three well-known algorithms with three different keys in a fixed order of sequence AES, Twofish, and Serpent. Steganography is used for securely transmitting this data to the receiver. This system performance lacks due to three cascaded encryption which performs Fiestel rounds as for AES -10, Twofish-32 and Serpent-32 in total 74 rounds of Fiestel structure are carried out for getting final results.

Priyanka and Lal, 2019 [22] had designed a hybrid model by mixing three algorithms in dynamic order using AES, DES, and Blowfish for big-data security. They marked their model as highly secure if all algorithms are used together for data confidentiality. They have remarked that the hybrid model AES-Blowfish is more secure than the DES-AES version.

There is enormous hybrid cryptographic techniques available, proposed by various researchers and implemented using numerous platforms, various simulation tools used for its performance analysis. Table 1 details a concise overview of various hybrid cryptographic techniques.

Authors	Algorithms Used	Model Description	Advantages	Disadvantages/ Remarks/ future work
Abdullah et al., 2018 [8]	IDEA and WAKE	Super-encryption algorithm utilizes IDEA and WAKE algorithms for double encryption where The IDEA encrypts and generates cipher text in ASCII form and WAKE first converts ASCII ciphertext into Hexadecimal before encryption process.	Requires longer time by cryptanalyst to break security.	Encryption process in mixed mode with parallelism No comparison provided with existing models.
Rachmawati et al., 2018 [11]	IDEA and Knapsack Algorithm	The plaintext is encrypted using IDEA algorithm and knapsack asymmetric key algorithm is used for secure distribution of the message key.	Maintains data integrity More secure	No comparison provided with existing models.
Tayel et al., 2018 [12]	Serpent and ECC	SEHC model uses Serpent algorithm for encrypting multimedia images and key sharing and distribution is handle by Elliptic Curve Cryptography (ECC) within an insecure communication channel.	system more reliable enhance Serpent key management protocol using ECC	shows potential for live application

Timilsina & Gautam, 2019 [13]	Blowfish and ECC	Random key generated and utilized by Blowfish algorithm for data encryption and key is encrypted using ECC for sharing.	multi-layer security hybrid is better than single algorithm	compared own models by varying key size
Venkatraman & Geetha, 2019 [14]	Blowfish and Genetic Operators	Blowfish encryption algorithm encrypts image information and then generic operators are you used for encrypting the already encrypted image information.	improved security than blowfish algorithm fast and ensures better security	improvements can be done by use of proxy-encryption with the high entropy and least correlation
Mahmud et al., 2018 [17]	AES and Blowfish	This model secures medical patient reports by encrypting them using hybrid model in sequence.	fixed order double encryption	Used RSA and ECC for Key generation, ECC works better.
Kaushik & Patel, 2019 [18]	AES and Twofish	The data owner encrypts his data before uploading it to cloud. The key will be shared by cloud service provider after user authentication.	fixed order double encryption	Model performs better than hybrid model AES + Blowfish developed by [23]
Neha, 2019 [19]	AES and Twofish	Model uses AES and Twofish for encrypting cloud data where ECDH is used for key management.	fixed order double encryption	Twofish key setup is fast and can also be used for smart cards.
Othman, 2017 [20]	RSA, Twofish and AES	Model used for securing communication with Robots.	Triple encryption.	Model requires more cryptanalysis time to brake using brute force method.
Priyanka & Lal, 2019 [22]	AES, DES and Blowfish	Model provides multiple variants by combining these algorithms for selection as per security requirement.	Dynamic Encryption	Highly secure if all three algorithms used.
Santoso et al., 2020 [24]	AES and Twofish	Model uses AES and Twofish for encrypting data with same key generated using SHA256 by providing passphrase.	fixed order double encryption	More secure and easier to implement.

Siva Sankaran & Kirubanand, 2019 [25]	Twofish and ECC	The plaintext is encrypted using Twofish algorithm and ECC asymmetric key algorithm is used for secure distribution of the secret key used by Twofish.	More secure	Slow in encryption and decryption for a large set of data.
Poduval et al., 2019 [26]	3DES, RC6 and AES	Divides data into three Parts- Each part is encrypted parallel using different algorithm based on key and key details stored and shared using image steganography technique.	Less processing time	Not discussed
Pooja & Chauhan, 2020 [27]	AES, DES and m-RSA	Divides data into three equal Parts- first part encrypted using AES; Second Part encrypted using DES and Third Part encrypted using m-RSA. The final ciphertext is C1C2C3.	More secure	Requires pre and post processing time.
Salama AbdElminaam, 2018 [28]	AES and Blowfish	Plaintext data partitioned into n block and each block further split in 2 parts; first part encrypted using AES and second part using blowfish.	More Secure	Block size not mentioned.
AbdElminaam et al., 2014 [29]	(AES and ECC) and (Blowfish and RSA)	This model does node encryption where plaintext divided in two equal parts first part is encrypted using AES and ECC algorithm and second part using Blowfish and RSA.	Fast Processing More Secure supports WSN applications	requires four algorithms
Kumar & Rana, 2016 [30]	modified AES	Plaintext encrypted using modified AES where fixed 16 rounds are used for single block of data.	More secure	Time Consuming due to additional rounds
Gupta et al., 2020 [31]	RSA and Blowfish	Plaintext Message M is first encrypted using Blowfish Algorithm and is used as a plain text for RSA algorithm. D-RSA algorithm is used for re-encryption.	Slow Processing more secure	Use triple RSA i.e. triple modulus based calculation using 6 prime numbers.

Ekka et al., 2019 [32]	AES and RSA	This hybrid model uses AES, RSA and EX-OR operation. The Plaintext M is encrypted using AES with secret key SK and then generated ciphertext and key SK are EX-ORed to generate intermediate ciphertext C2. The RSA encrypts SK which is EX-ORed with C2 to generate final ciphertext C3.	Less processing time than AES-256	No use/need to perform EX-OR operation on C2 and SK' to generate C3.Since, sender has to send C3 along with SK' which gives C2, if C3 EX-OR with SK'.
Saxena et al., 2020 [33]	RSA, Elgamal and MD5	A Hybrid Model REM first encrypts the plaintext using Elgamal algorithm and then re-encrypted using RSA algorithm. MD5 is used for message digest.	Double encryption	Results are generated based on small size data

Table 1 Overview of Various Hybrid Cryptographic Techniques

3. PROPOSED METHODOLOGY

The proposed system produce a hybrid algorithm based on cascading of modified versions of different symmetric algorithms. The hybrid models use the proposed scheme and perform multiple encryptions with different keys used for each cascading algorithm with a modified internal structure. The proposed system is implemented using the famous open-source Crypto++ [34] library which is developed using the C++ class library and provides cryptographic schemes. Most of the cryptographic algorithm has fixed number of rounds which is hardcoded in its code, and very few algorithms rounds are calculated based upon the size of the key. Table 2 provides the details of the algorithm whose code has been modified with a new number of rounds as per the table in the Crypto++ library without affecting its execution.

Sr. No.	Algorithm Name	Key Size (bits)	No. of Rounds (Existing)	No. of Rounds (Modified)
1	AES (Rijndael)	128	10	4
2	DES	64	16	1
3	Blowfish	128	16	1
4	Twofish	128	32	2
5	Serpent	128	32	8

Table 1 Algorithms Description with Modified no of Rounds Used for Hybrid Model

3.1. Generalized Model Architecture

Figure 2 depicts the encryption-decryption process of a hybrid model with a modified internal structure of algorithms. The encryption process (shown in fig from left to right) involves cascading of numerous algorithms with a modified number of rounds and keys generated using SHA256 of different passphrases. The decryption process (shown in figure 2 from right to left) is exactly the reverse process of encryption.

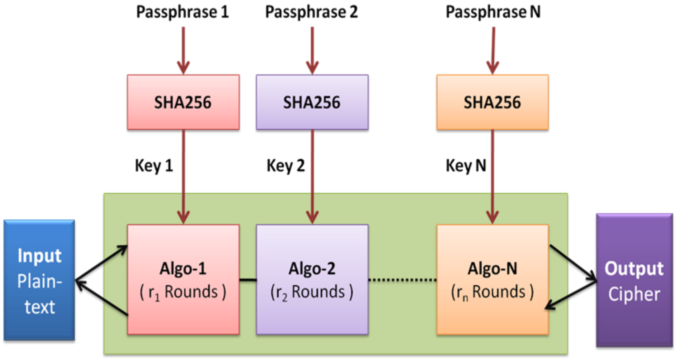

Figure 2 Generalised Hybrid Model Architecture

3.2. Flowchart of the Proposed Scheme

Figure 3 represents the flowchart of the proposed scheme which can be applied on any hybrid model which uses multiple or cascaded encryptions. For explaining the proposed scheme in detail, we select the hybrid model TWOFISH-AES. Plaintext file is given as input along with two passphrases which will be utilized for Key and IV generation. The proposed model firstly encrypts the plaintext file with TWOFISH algorithm having 2 rounds whose key and IV generated using SHA256 algorithm by taking passphrase-1. The output of the first step is then again encrypted using AES algorithm whose key and IV are generated using SHA256 algorithm by taking passphrase-2 having 4 rounds and generates final ciphertext file.

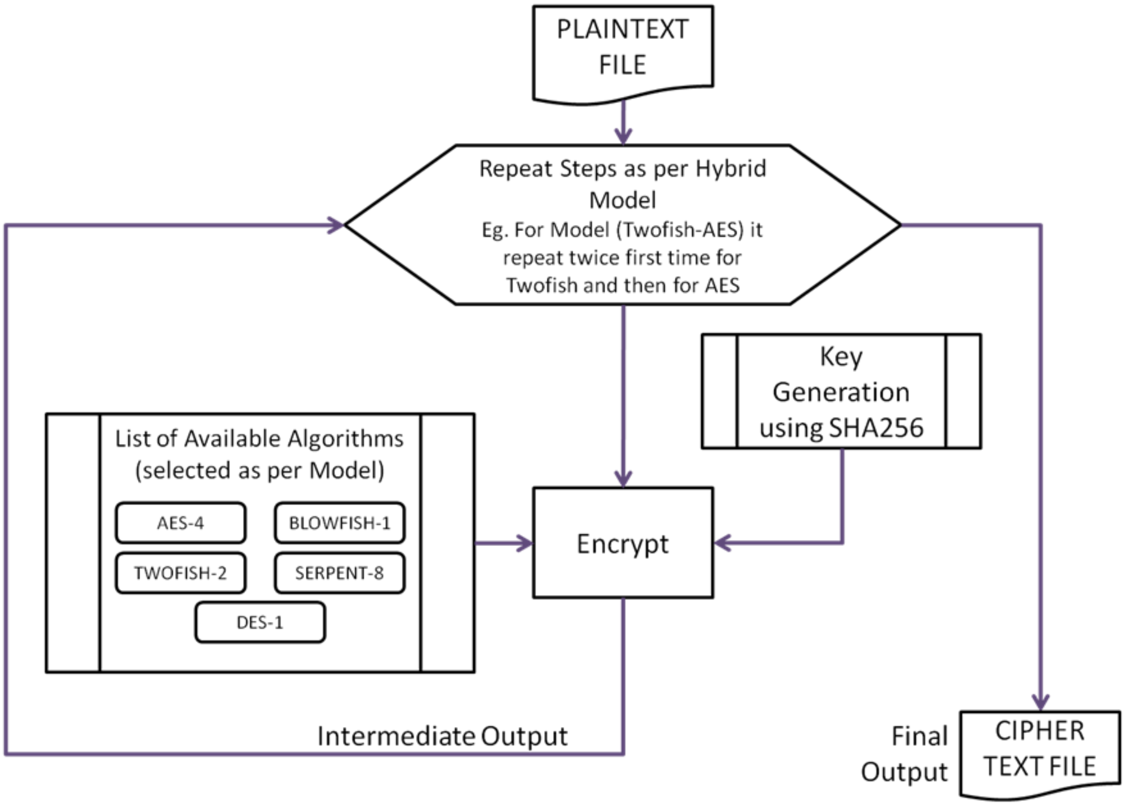
PLAINTEXT FILE
Repeat Steps as per Hybrid Model
Eg. For Model (Twofish-AES) it repeat twice first time for Twofish and then for AES
Key Generation using SHA256
List of Available Algorithms (selected as per Model)
AES-4
BLOWFISH-1
TWOFISH-2
SERPENT-8
DES-1
Encrypt
Intermediate Output
Final Output
CIPHER TEXT FILE

Figure 3 Flowchart of the Proposed Model using Internal Structure Modification Scheme

The key generation algorithm generates n different keys for the hybrid model using the SHA256 algorithm as per the need of the algorithm which is used in the encryption and decryption process. The secret key is independent for each algorithm and generated using the SHA256 algorithm using a different passphrase for maintaining security level. The key and IV (Initial Vector) generation for each algorithm can be given by eq. 1 and eq. 2 respectfully as

$$Key_i = Trunc\ (\ H\ (Passphrase_i),\ B_i) \quad i = 1\ to\ n \quad (1)$$

$$IV_i = Trunc\left(\ H\left(H\ (Passphrase_i)\right),\ V_i\right) \quad i = 1\ to\ n$$
(2)

Where,

$Trun()$ - truncates the input to given size

$H()$ - SHA256 Algorithm

$Passphrase_i$ - passphrase used for key generation for ith algorithm

B_i - Size of key for ith algorithm

V_i - Size of IV for ith algorithm

Eq. 3 represents the mathematical equation for encryption process performed by proposed cipher scheme with modified number rounds for n-level of cascading which utilizes keys and IVs generated using Eq.1 and Eq.2 where Ci represents the ciphertext generated with ith algorithm in the selected model with rounds specified in table 2. Eq. 4 represents the decryption process of the proposed scheme for hybrid models.

$$C_i = \begin{matrix} P & i = 0 \\ E_i\ (\ Key_i,\ IV_i,\ C_{i-1}, r_i) & i = 1\ to\ n \end{matrix} \quad (3)$$

$$P_{i-1} = \begin{matrix} C_n & i = n+1 \\ D_i\ (\ Key_i,\ IV_i,\ P_i, r_i) & i = n\ to\ 1 \end{matrix} \quad (4)$$

Where,

C_i - Cipher text of ith Algorithm

E_i - Encryption using ith Algorithm

D_i - Decryption using ith Algorithm

Key_i - Key for ith Algorithm

IV_i - IV ith Algorithm

r_i - number of rounds used for encryption algorithm

P_{i-1} - recovered plaintext using ith Algorithm

P, C_n - Initial Plaintext and Final Ciphertext

4. RESULT ANALYSIS

Result analysis involves the comparison of existing hybrid models with prescribed number of rounds with modified number of rounds for same model in terms of encryption time, encryption and decryption throughput for varying size of text and image files as per details given in table 3.

Hybrid model involving symmetric encryption only	Total number of rounds performed in existing model	Total number of rounds performed in modified model
AES-BLOWFISH [17]	36	5
AES-TWOFISH [18], [19], [24]	42	6
TWOFISH-AES [20]	42	6
AES-TWOFISH-SERPENT [21]	74	14
AES-BLOWFISH-DES [22]	46	6

Table 2 Hybrid Cipher Model with Number of Rounds Performed During Process

4.1. Encryption Time

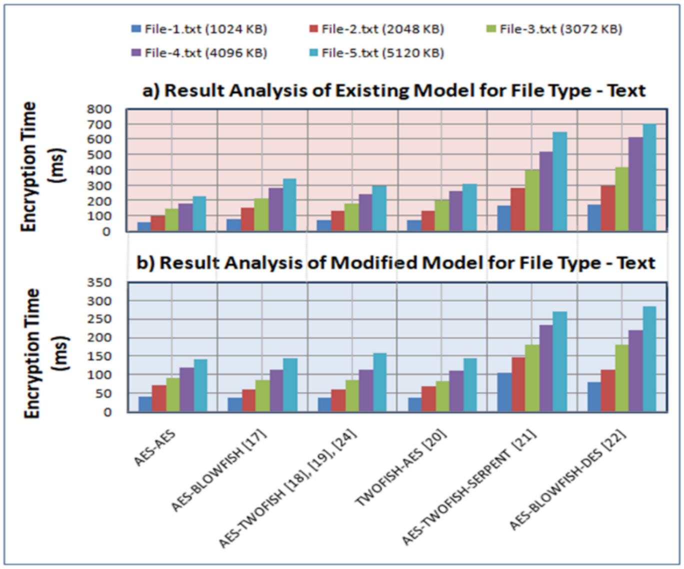

Figure 4 Encryption Time Required by Existing and Modified Hybrid Model for Text Files

It denotes the time required by the cryptographic model for the encryption process i.e. converting plaintext into the ciphertext. Figure 4 shows the graphical representation of encryption time required by hybrid models for converting plaintext into the ciphertext for text files of different sizes. Figure 4 a) shows time required by the existing hybrid models whereas Figure 4 b) shows the time required by modified hybrid models.

Figure 5 shows the graphical representation of encryption time required by hybrid models for converting plaintext into the ciphertext for image files of different sizes. Figure 5 a) shows time required by the existing hybrid models whereas Figure 5 b) shows the time required by modified hybrid models.

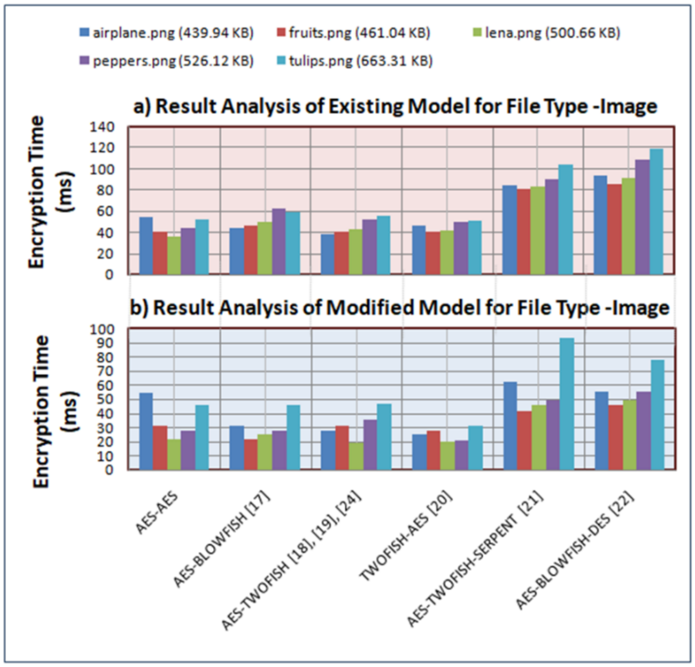

Figure 5 Encryption Time Required by Existing and Modified Hybrid Model for Images

Comparing Figure 4a with Figure 4b and Figure 5a with Figure 5b, we can conclude that modified hybrid models with proposed scheme takes lesser time than its corresponding existing hybrid models. We have observed significant improvement in time performance in terms of encryption time for proposed scheme for all modified hybrid models having a reduced number of rounds.

4.2. Decryption Time

It denotes the time required by the cryptographic model for the decryption process i.e. converting ciphertext into the plaintext. Figure 6 and Figure 7 shows the graphical representation of decryption time required by hybrid models for converting ciphertext into the plaintext for text and image files of different sizes respectively. We have observed improvement in performance for proposed scheme in hybrid models for decryption process too.

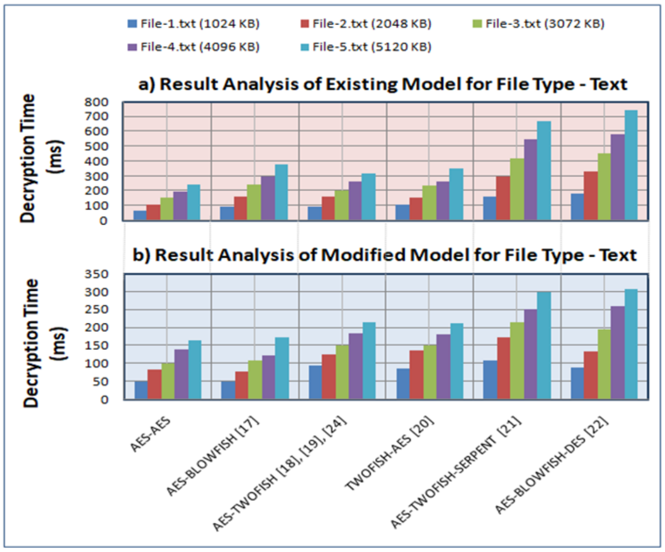

Figure 6 Decryption Time Required by Existing and Modified Hybrid Models for Text Files

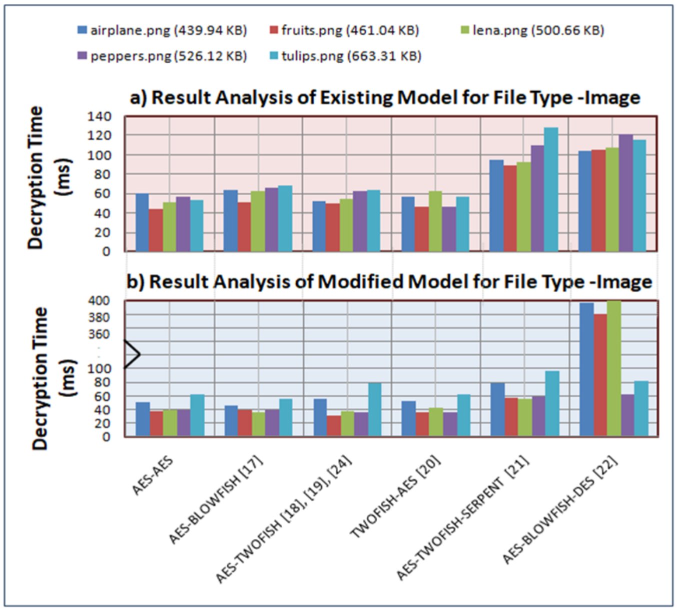

Figure 7 Decryption Time Required by Existing and Modified Hybrid Models for Images

4.3. Encryption Throughput

It denotes the average speed of the cryptographic model for the encryption process i.e. amount of plaintext converted to the ciphertext in unit time. Figure 8 shows the graphical representation of encryption throughput of the various existing hybrid model and proposed modifications in the existing model for encrypting text and image files. The result shows the improvement in encryption throughput for all proposed hybrid models with a reduced number of rounds.

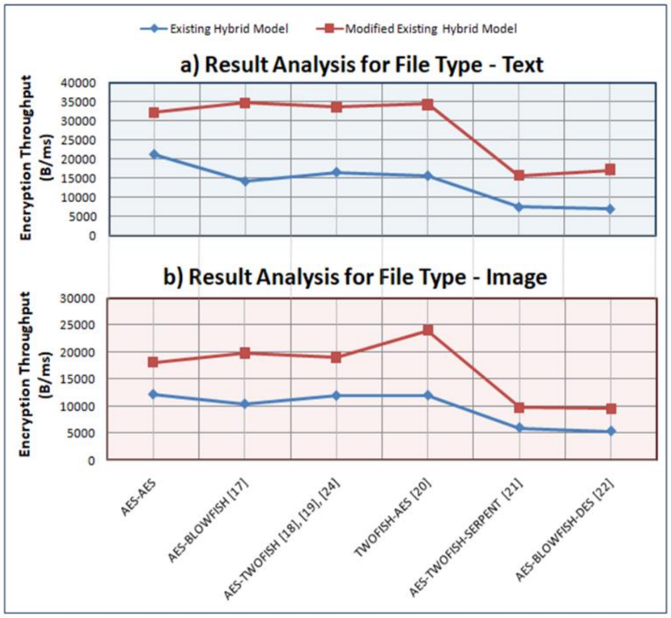

Figure 8 Average Encryption Throughput of Existing and Proposed Hybrid Model

4.4. Decryption Throughput

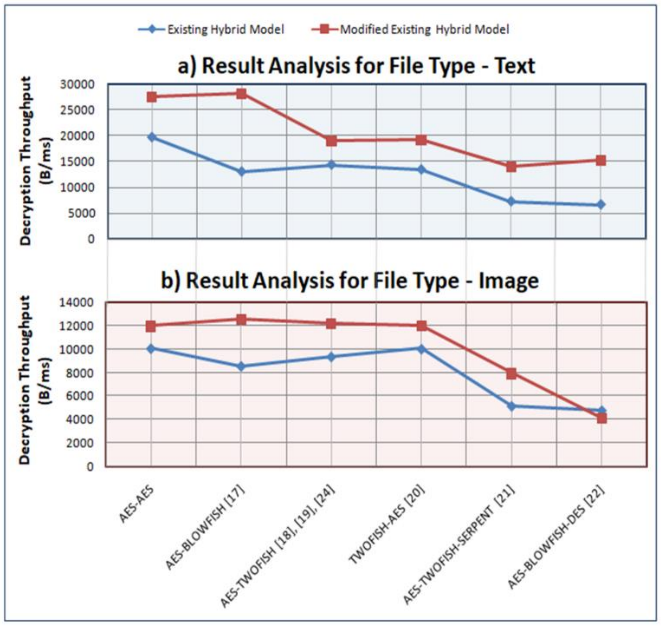

Figure 9 Average Decryption Throughput of Existing and Proposed Hybrid Model

It denotes the average speed of the cryptographic model for the decryption process i.e. amount of ciphertext converted to plaintext in unit time. Figure 9 shows the graphical representation of decryption throughput of the various existing hybrid model and proposed modifications in the existing model for decrypting text and image files. The result shows the improvement in decryption throughput for the proposed hybrid model with a reduced number of rounds.

5. CONCLUSION AND FUTURE WORK

This work concludes that the proposed hybrid cipher scheme with a reduced number of rounds improves the performance of the hybrid cascaded model by maintaining a minimum level of security using the different secret keys used for each cascaded encryption algorithm generated using the SHA256 algorithm. The modified hybrid model TWOFISH-AES has the best performance considering encryption throughput as per fig. 8, which gives the average speed of 34301.43 b/ms for text files and 23950.44 b/ms for images. The proposed hybrid cipher scheme can be integrated into any application which requires a faster way of preserving the security of user's personal files like text, images, etc. The security level of this hybrid cipher scheme can further be increased by using a dynamic selection of algorithms instead of the fixed order of algorithms for the encryption and decryption process in the hybrid cascaded model. The proposed design can also be implemented for other multimedia data like audio or video files types like .mp3, .avi, etc. The proposed concept can be incorporated in any application where high system performance is required like big data websites, cloud applications, or chatting applications.

REFERENCES

[1] M. M. Hoobi, "Efficient Hybrid Cryptography Algorithm," J. Southwest Jiaotong Univ., vol. 55, no. 3, Jun. 2020, doi: 10.35741/issn.0258-2724.55.3.5.

[2] P. Soni and R. Malik, "Performance Analysis of Cascaded Hybrid Symmetric Encryption Models," Turkish J. Comput. Math. Educ., vol. 12, no. 2, pp. 1699–1708, Apr. 2021, doi: https://doi.org/10.17762/turcomat.v12i2.1506.

[3] Eman Salim Ibrahim Harba, "Secure Data Encryption Through a Combination of AES, RSA, and HMAC," Eng. Technol. Appl. Sci. Res., vol. 7, no. 4, pp. 1781–1785, 2017.

[4] G. Marinakis, "Modification and customization of cryptographic algorithms.," J. Appl. Math. Bioinforma., vol. 9, no. 1, pp. 1–13, 2019.

[5] W. Stallings, Network Security Essentials, Fourth Edi. Prentice Hall Press, USA, 2010.

[6] F. J. D'souza and D. Panchal, "Advanced encryption standard (AES) security enhancement using hybrid approach," Proceeding - IEEE Int. Conf. Comput. Commun. Autom. ICCCA 2017, pp. 647–652, 2017, doi: 10.1109/CCAA.2017.8229881.

[7] B. Schneier, Applied Cryptography, Second Edi. John Wiley & Sons, Inc, 1996.

[8] D. Abdullah et al., "Super-Encryption Cryptography with IDEA and WAKE Algorithm," J. Phys. Conf. Ser., vol. 1019, no. 1, 2018, doi: 10.1088/1742-6596/1019/1/012039.

[9] A. Akhavan, A. Samsudin, and A. Akhshani, "Cryptanalysis of 'an improvement over an image encryption method based on total shuffling,'" Opt. Commun., vol. 350, pp. 77–82, 2015, doi: https://doi.org/10.1016/j.optcom.2015.03.079.

[10] H. Noura, L. Sleem, and R. Couturier, "A revision of a new chaos-based image encryption system: Weaknesses and limitations," arXiv, 2017.

[11] D. Rachmawati, M. S. Lydia, and W. A. Siregar, "Hybrid Cryptosystem Implementation Using IDEA and Knapsack Algorithm for Message Security," J. Phys. Conf. Ser., vol. 1090, no. 1, 2018, doi: 10.1088/1742-6596/1090/1/012030.

[12] M. Tayel, G. Dawood, and H. Shawky, "A Proposed Serpent-Elliptic Hybrid Cryptosystem for Multimedia Protection," 2018 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2018, no. September 2018, pp. 387–391, 2018, doi: 10.1109/ICACCI.2018.8554950.

[13] S. Timilsina and S. Gautam, "Analysis of Hybrid Cryptosystem Developed Using Blowfish and ECC with Different Key Size," Tech. J., vol. 1, no. 1, pp. 10–15, 2019, doi: 10.3126/tj.v1i1.27582.

[14] K. Venkatraman and K. Geetha, "Dynamic virtual cluster cloud security using hybrid steganographic image authentication algorithm," Automatika, vol. 60, no. 3, pp. 314–321, 2019, doi: 10.1080/00051144.2019.1624409.

[15] H. Abroshan, "A Hybrid Encryption Solution to Improve Cloud Computing Security using Symmetric and Asymmetric Cryptography Algorithms," Int. J. Adv. Comput. Sci. Appl., vol. 12, no. 6, pp. 31–37, 2021, doi: 10.14569/IJACSA.2021.0120604.

[16] M. Hussam, G. H. Abdul-majeed, and H. K. Hooomod, "New Lightweight Hybrid Encryption Algorithm for Cloud Computing (LMGHA-128bit) by using new 5-D hyperchaos system," Turkish J. Comput. Math. Educ., vol. 12, no. 10, pp. 2531–2540, 2021.

[17] A. H. Mahmud, B. W. Angga, Tommy, A. E. Marwan, and R. Siregar, "Performance analysis of AES-Blowfish hybrid algorithm for security of patient medical record data," J. Phys. Conf. Ser., vol. 1007, 2018, doi: 10.1088/1742-6596/1007/1/012018.

[18] S. Kaushik and A. Patel, "Secure Cloud Data Using Hybrid Cryptographic Scheme," Proc. - 2019 4th Int. Conf. Internet Things Smart Innov. Usages, IoT-SIU 2019, pp. 1–6, 2019, doi: 10.1109/IoT-SIU.2019.8777592.

[19] P. Neha, "Implementation of Hybrid AES And TWOFISH For Cloud," J. Gujarat Res. Soc., vol. 21, no. 6, pp. 664–682, 2019.

[20] S. Othman, "Securing Robotic Communication using Multiple Security Techniques," Int. J. Comput. Appl., vol. 178, no. 1, pp. 1–4, 2017, doi: 10.5120/ijca2017915704.

[21] M. M. Rajan and A. James, "Hiding Encrypted Text Files In Multimedia Files," Int. J. Eng. Res. Technol., vol. 2, no. 3, pp. 1–10, 2013.

[22] G. Priyanka and A. M. Lal, "A hybrid encryption method handling big data vulnerabilities," Int. J. Cloud Comput., vol. 8, no. 3, pp. 207–213, 2019, doi: 10.1504/IJCC.2019.103879.

[23] S. Kaushik and C. Gandhi, "Cloud data security with hybrid symmetric encryption," 2016 Int. Conf. Comput. Tech. Inf. Commun. Technol. ICCTICT 2016 - Proc., pp. 636–640, 2016, doi: 10.1109/ICCTICT.2016.7514656.

[24] K. I. Santoso, M. A. Muin, and M. A. Mahmudi, "Implementation of AES cryptography and twofish hybrid algorithms for cloud," J. Phys. Conf. Ser., vol. 1517, no. 1, 2020, doi: 10.1088/1742-6596/1517/1/012099.

[25] P. Siva Sankaran and V. B. Kirubanand, "Hybrid cryptography security in public cloud using TwoFish and ECC algorithm," Int. J. Electr. Comput. Eng., vol. 9, no. 4, pp. 2578–2584, 2019, doi: 10.11591/ijece.v9i4.pp2578-2584.

[26] A. Poduval, A. Doke, H. Nemade, and R. Nikam, "Secure File Storage on Cloud using Hybrid Cryptography," Int. J. Comput. Sci. Eng., vol. 7, no. 1, pp. 587–591, Jan. 2019, doi: 10.26438/ijcse/v7i1.587591.

[27] Pooja and R. K. Chauhan, "Triple phase hybrid cryptography technique in a wireless sensor network," Int. J. Comput. Appl., 2020, doi: 10.1080/1206212X.2019.1710342.

[28] D. Salama AbdElminaam, "Improving the Security of Cloud Computing by Building New Hybrid Cryptography Algorithms," I.J. Electron. Inf. Eng., vol. 8, no. 1, pp. 40–48, Mar. 2018, doi: 10.6636/IJEIE.201803.8(1).05.

[29] D. AbdElminaam, H. M. Abdul Kader, M. M. Hadhoud, and S. M. El-Sayed, "Developing and Evaluation of New Hybrid Encryption Algorithms," Int. J. Comput. Technol., vol. 13, no. 1, pp. 4038–4052, 2014, doi: 10.24297/ijct.v13i1.2926.

[30] P. Kumar and S. B. Rana, "Development of modified AES algorithm

for data security," Optik (Stuttg)., vol. 127, no. 4, pp. 2341–2345, 2016, doi: 10.1016/j.ijleo.2015.11.188.

[31] A. Gupta, S. Gupta, and N. Yadav, "Enhancement of security using B-RSA algorithm," in Lecture Notes in Networks and Systems, vol. 89, Springer, 2020, pp. 439–450.

[32] D. Ekka, M. Kumari, and N. Yadav, "Enrichment of Security Using Hybrid Algorithm," in Lecture Notes on Data Engineering and Communications Technologies, vol. 15, Springer Singapore, 2019, pp. 867–873.

[33] P. Saxena, S. Yadav, and N. Dayal, "Hybrid approach to enhance data security on cloud," Lect. Notes Networks Syst., vol. 89, pp. 735–743, 2020, doi: 10.1007/978-981-15-0146-3_69.

[34] W. Dai, "Crypto++ Library 8.2 | Free C++ Class Library of Cryptographic Schemes." [Online]. Available: https://www.cryptopp.com/. [Accessed: 10-May-2021].

Authors

Pravin Soni is a research scholar in Computer Science and Engineering department at LPU, Punjab and has pursued his M. Tech (Computer Engg.) from Veermata Jijabai Technological Institute, Mumbai in 2011. His research interest covers algorithm, network and security.

Rahul Malik (Member, IEEE) received the M.Tech. degree from NIT Nagpur and the Ph.D. degree from NIT, Jalandhar, Punjab, in 2019. He has expertise in teaching, research and development of seven years. He has more than ten research articles along with book chapters, including more than five articles in SCI indexed journals. His research interests include machine learning, deep learning, image processing, and soft computing.

How to cite this article:

Pravin Soni, Rahul Malik, "Efficient Cipher Scheme for Hybrid Models with Internal Structure Modification", International Journal of Computer Networks and Applications (IJCNA), 8(5), PP: 596-606, 2021, DOI: 10.22247/ijcna/2021/209990.