Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 7s (2024)

A Novel AFR Encryption Algorithm for Secure Data Transmission

[1]S.Muthusundari, [2]M.D.Vimalapriya, [3]N.Umamaheswari, [4]V.Devi, [5]Seemantula Nischal

[1]Associate Professor, Department of Computer Science & Engineering, R.M.D. Engineering College, Kavaraipettai, India. sms.cse@rmd.ac.in

[2]Assistant Professor, Department of MCA, MEASI Institute of Information Technology, Chennai, India. vimalapriya.md@measiit.edu.in

[3]Assistant Professor, Department of Computer science and Engineering, Sir.M.Visvesvaraya Institute of Technology, Bangalore, India. umamaheswari_cs@sirmvit.edus

[4]Assistant Professor, Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology, Coimbatore, India. devivenkataswamy@gmail.com

[5]Masters in Computer Science, State University of New York, Buffalo, United States. Nischal200216@gmail.com

Article History:

Received: *01-06-2024*

Revised: *03-07-2024*

Accepted: *29-07-2024*

Abstract:

Cryptographic analysis is always a fascinating field of research. It is understood that data security is the major concern in the Internet world. The process of encryption and decryption are cryptographic that are intended to provide data confidentiality over the network. Currently more number of organizations is working on huge databases in the real world to attain the best efficient data transfer security mechanism. Only information security can be maintained by conventional encryption methods. Data can be accessed by an unauthorized client for malicious purposes. Efficient encryption and decryption methods should be used to improve data security. The Proposed AFR Algorithm deals with 3 levels, namely Append, Formation of BST and Representation of Matrix which provides a strong encryption to provide security for transmission of data. This proposed novel AFR encryption algorithm creates the complexity in encryption to a huge extent; hence security is high in transmission of data.

Keywords: Append, BST, Matrix, Security, Complexity

1. Introduction

The current world is integrated with internet to a greater extent. Internet is only the media connecting people across the world[1]. While connecting people through the internet, there is a need for security of their data transferred during communication. Secure pathways for communicationplay a vital role in connecting people around the world.The term Cryptology is a technique to provide security to the data while transmitting data from sender to receiver [2]. There are many ways to use the internet to transmit data: through e-mails, chats, using various platforms,etc[3].The data transfer made using the internet is very quick and accurate[4]. The "security threat" it poses, i.e. personal or private data that is bagged or compromised in many ways, is one of the main challenges of sending data over the internet. Hence, taking data security into account becomes very important, as it is one of the most critical considerations that need attention during the data transfer process.

Security plays a vital role in storage and transmission of information across undefined networks in a secure manner.Cryptography is a key component of secure communication and transmission of information for security services such as confidentiality, data integrity, access control, authentication and non-repudiation. This provides a means of preserving sensitive information by transmitting it in unintelligible form and providing provisions for licensed recipient alone to access this information by translating it to original text. The method of converting plain text to cipher text with a key is called the encryption process and reversal the encryption process is called

the decryption process[5]. The design of cryptographic algorithms is to be safe and efficient, low cost, requires a small memory footprint, is easy to implement and can be used on multiple platforms. A wide range of applications have been developed to secure cryptographic algorithms using different mathematical processes.

To overcome this disparity issues, in this paper a novel AFR encryption algorithm is suggested using append and matrix approach. The contribution of this research paper is summarized as in a consecutive manner

a) Providing a new strategy for encryption and decryption using append and matrix
b) Providing two levels of encryption
c) Increasing the security level of encryption and decryption

The Structure of this novel AFR algorithm paper is as follows. Section 2 Discusses about the related work of various encryption and decryption algorithm process using Binary search and matrix based approaches. Section 3 deals about the proposed AFR methodology and architecture of the proposed algorithm, Section 4 concentrates in results and discussions, and follows the conclusion and references section.

2. Literature Review

A new block cipher encryption algorithm was proposed by Rajni Jain and Ajit Shrivastava [6]. Their approach was implemented with logical functions, like XOR operations, circular shift and mathematical calculations to perform encryption and decryption process. Their method was compared with the standard existing algorithms like modified Hill cipher and a block cipher with one key, and concluded that their method had better performance in various parameters such as avalanche effect and utilization of memory on various size text files. In order to achieve higher level security, they will have a future plan to increase the number of logical operations.

Multilevel phase of Encryption was presented by Himanshu Gupta and Vinod Kumar Sharma [7] . In their research work the input text data is encrypted multiple times with strong keysat each level of phases. It wasa strong technique for data transmission & information security and it takes part an important role in modern Cryptographic world. It was describing the enhanced complexity of data encryption due to multiple levels of operations of single phase encryption techniques in cryptography. The advantage of this approach is that it providesa safe environment for better security because even if some component ciphers are broken or some of the secret keys are recognized, the confidentiality of original data can still be maintained by the multiple levels of encryptions. The implementation of multilevel phase encryption is a safe, strong and positive move towards in the way of defining a standard for network security.

A new encryption and decryption algorithm using 2D Matrices have proposed by Balaji Maram et.al [8]. They were maintaining 2 keys, one is permanent as shared key and other is temporary as session key of both 16 byte lengths from sender to receiver. Temporary keys were valid for specific session only. Based on these two keys an intermediate key was generated in 4*4 matrix format. Matrix entries were shuffled by the concept of Double-reflecting-data-perturbation method to encrypt the input text. In the decryption process, the matrix entries was transposed, reshuffled and by Double reflecting data perturbation method the original input was attained.

An Improved Cryptographic Technique for the encryption of text message using double encryption has presented by Yashpalsingh Rajput et al [9]. Two phases of encryption were introduced in this research work. The first phase is improved substitution cipher and the second phase is hill cipher technique. Due to this two phases a strong encryption is created and even brute force attackers also unable to break the original text. Hence they have defined a strong security level in their paper.

An optimized encryption technique by an arbitrary matrix with probabilistic encryption algorithm has proposed by Paresh Ratha et.al [10]. This research paper is applied arbitrary matrix key for initial vector. The encryption and decryption is performed with ASCII substitution and had significance of creating poly alphabet ciphers with

probabilistic encryption. The experiment was conducted and compared with other existing algorithms. Theperformances of their arbitrary algorithms areexamined based on parameters like, execution time, throughput and Avalanche effect with DES, AES and Blowfish. The result of this algorithm is better than Blowfish algorithm.

A new AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection have described by Nishtha Mathur and Rajesh Bansode [11]. They have used 2 algorithms for the text encryption. One is AES used to encrypt the original text. Then ECC algorithm is used to encrypt the AES text. Two way encryption policies are applied to prevent data from vulnerability. Their study was focused to increase the key size from 128 bits to the maximum key size 192 bits and in 12 round iterations.

A New variant of Hill Cipher Algorithm for Data Security has described by Kalaichelvi V, Manimozhi K, Meenakshi P, Rajakumar B, Vimaladevi P [12]. This paper recommends converting any text, digits and special symbols. The plain message is converted into 64 bit radix characters using 64 bit radix encoding method. Then again the encrypted message is converted into Hill cipher algorithm to create cipher text. Similarly for decryption process radix 64 bit decoding concept is introduced. Hence it improves the complexity in encryption process.

A new encryption algorithm and a new architecture for data encryption and decryption was proposed by Prof. Swapnil Chaudhari1, Mangesh Pahade et.al[13]. This study dealt the advantages of the architecture over past cryptography algorithm and tool to meet High security, Un-easy decryption and High efficiency.

Anew cryptographic encryption technique called Spiral Rotation. This algorithm is based on the matrix representation pattern has presented by S Sanal Kumar and S. Anfino shefrin [14]. The spiral rotation is performed by change the data into a parallel sequence of matrices containing converted and shuffled numeric, and performs rotation about the diagonal entries so that the process of the encryption time is reduced and encryption steps are minimized.

A new enhanced algorithm using three phase protocols has proposed by Syed Tariq Shah Waqif [15]. They have designed three times authentication process from sender to receiver. During this phase XOR operation is processed to encrypt the data.

A new Analysis of Combination Algorithm Data Encryption Standard (DES) and Blum-Blum-Shub (BBS) has been proposed by O Laia , E M Zamzami and Sutarman [16]. In their paper, they have Combined the DES algorithm with the Pseudo-random number generator Blum-BlumShub (BBS) to produce external keys in the encryption and decryption process of messages, that performs a unique key and a good level of security initiated.

A new Complex Encryption System Design Implemented by AES has been proposed by Zhimao Lu, Houmed Mohamed [17]. They focused on the systematic analysis and issues of the key management and security issues. They used to reduce round key and improve key schedule for analyzing the performance of the proposed method.

3. Proposed Methodology

The proposed algorithm AFR is different from existing methodology to provide security encryption for transmission of data.It creates the complex encryption process for the plain text and performs various operations with different encryption key and develops encrypted data. The algorithm is dealt with three levels namely,

1. Append Function (Prefix & Suffix)
2. Formation of Binary Search Tree
3. Representation of Matrix

The proposed algorithm provides security at three levels of encryption and decryption process. In first level, it appends the prefix and suffix character of each and every character in the plain text or the given original data text. In the second level it forms the binary search tree for the appended plain text. Then it performs in-order tree traversal from the Binary search tree that shows the cipher text.

To perform decryption process, the cipher text is represented as a 3*M matrix format which is considered as the third level of security of this proposed method. In this decryption process, the column order of the matrix to be calculated by the formula

$$M= N/3 \quad (1)$$

where N is the number of intermediate characters in the cipher text (Encrypted data). Once the order of the column is derived (M), then the encrypted characters are represented in the 3*M matrix format. The 3 row entries are identified as R1,R2 and R3. The M column matrices are identified as special characters C1, C2, C3 and CM respectively. To decrypt the encrypted text it is necessary to calculate the location for each and every letter in the cipher text which is retrieved from the matrix format. The formula is derived to identify the each letters location from the matrix table. The first letter of the cipher text is in C2 location. Then calculate the remaining locations are derived by the formula

E(Wi) = b= 2 (C2 location hence assumed as 2 for first character)

b +3 >= M-1 then Location K(1,b)

(b +3 <= M*2) && (η +3 > M -1) the location K(2,b)

elseit is in the location K(3,b)

Finally all the locations of the cipher text are identified and original plain text is achieved.

The main advantage of this proposed algorithm is provided with higher security and unable to find the original text input data by the brute force attackers. The implementation flow of the proposed AFR algorithm is depicted in the following figure 1.

Encryption Algorithm

1. Get the Plain text
2. Append prefix and suffix value to each character in the plain text
3. Form the binary search tree for each character after appending prefix and suffix value
4. Write the intermediate text in In-order tree traversal.
5. The Cipher text E(η) = intermediate text in In-order tree traversal.

Decryption Algorithm

1. Get the encrypted data.
2. Represent the intermediate text by matrix format using calculations based on the number of characters in the intermediate text. The formula for N intermediate characters M=N/3 then construct 3*M Matrix. Write the intermediate characters in the matrix.
3. For decrypting process, the first letter is in β location hence M(1,β)

To calculate the location,

E (Wi) = b = 2 (C2 location hence assumed as 2 for first character)

b +3 >= M-1 then Location K(1,b)

(b +3 <= M*2) && (η +3 > M -1) the location K(2,b)

	else it is in the location K(3,b)
4.	Original Plain text E(Wi), the number of characters in plain text is equivalent to M Characters.

3.1 Architecture Diagram of the Proposed Methodology

This research paper has focused on a new approach for Secured Encryption of Data Transmission using a novel AFR approach. Many people are transmitting their information from one user end to other user end in day to day life, so it is very essential to deal with the security of the sender's information. To meet out the security constrains, in this proposed research paper a novel AFR encryption algorithm has been implemented. The architecture diagram of novel proposed AFR algorithm is shown in figure. 1.

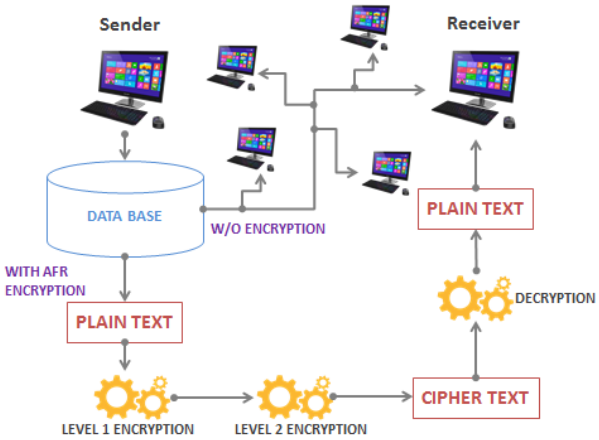


Figure 1 Architecture Diagram of Novel Proposed AFR Algorithm

There are many users are attached in the Internet. Whenever the users need to transmit their information to any other users, they can send their message to the particular recipient in a secured manner by encrypting their data,So that a secure transmission is possible between the sender and receiver in the internet. For maintaining a safe and secure environment for transmission of data, in this paper a novel AFR encryption algorithm is implemented. This algorithm provides two levels of security in encryption and additional one level security process in decryption process. Whenever the sender has to send the plain text to receiver,in the first level, append function is implemented by adding prefix and suffix character of each and every elements in the plain text. Then in the second level security of encryption Binary search tree is constructed for the first level intermediate data of the plain text. Then the in-order representation of the Binary search tree is derived which is called the Cipher text. The sender's information is now encrypted and cipher text is transmitted to the receiver end with the secret key. To decrypt the cipher text data, the Cipher text is represented in 3*M Matrix which provides the third level of security, Then to form the original plain text, formula is applied to identify the location in the matrix considering various cases. The result of the decryption shows the original plain text.

3.2 Encryption Process

The Proposed algorithm works as follows. The sender S and the receiver R share the matrix key, for the process of encryption and decryption. The process of encryption is done in two levels. In level 1, for each and every character in the original input data it appends the prefix and suffix of every letter. If the first letter is b, then it appends prefix of b as b-1 and suffix of b as b+1. Similarly, all the characters of the original input data are appended in such a manner. In the second level the binary search tree is constructed of the appended text. The two levels of the encrypted data is shown in the following figure 2. To encrypt the original input data (P), S

applies with prefix and suffix of each letter in M, a-1 <a <a+1; and constructs binary search tree in the manner a-1 <a <a+1.Then the cipher text is calculated as

$$C(x) = x.prefix(x).suffix(x) + \sum_{x=1}^{n}(BST(x-1).BST(n-x)) \qquad (2)$$

The cipher text is now transmitted to the receiver R. The two levels of encryption is found in the figure 2. The one level of decryption process is found in figure 3.

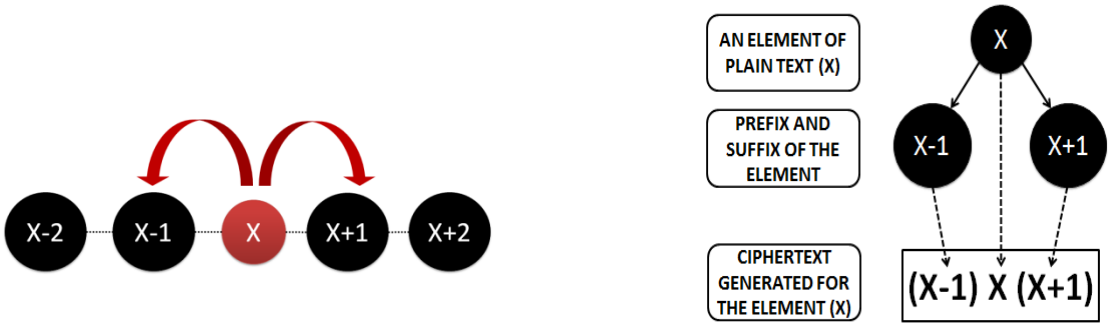


Figure 2. First and Second level of Encryption Process

3.3 **Decryption Process.**The encrypted text is now transmitted to the receiver R. The encrypted text C has to be represented in 3*M matrix format. All the cipher text C are aligned in the matrix representation as K(a,b) where a= 1,2,3 and b= 1,2,3,…..M. After representation of all the elements in the matrix, the decryption is done by calculating the locations. The location of the first element K(a,b) is identified; The value of a=1 and b=2 for the first element in all the cases. And to identify as next location, the index of K(a,b) which is b is found (b=2 in case of first element). The next location is found by the formula K(a,b + 3) if (b+3) >=M-1then the location is K(1,b+3), if (b+3) <= M*2 & (b +3) > M -1) the location K(2,b+3) else the location is K(3,b+3). After getting the location of all the elements in the matrix through the above method, the plain text is formed

4. Testing and Implementation of Proposed Methodology

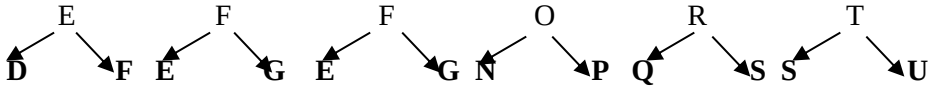
4.1 Encryption Process

Let us take the plain text **EFFORT**

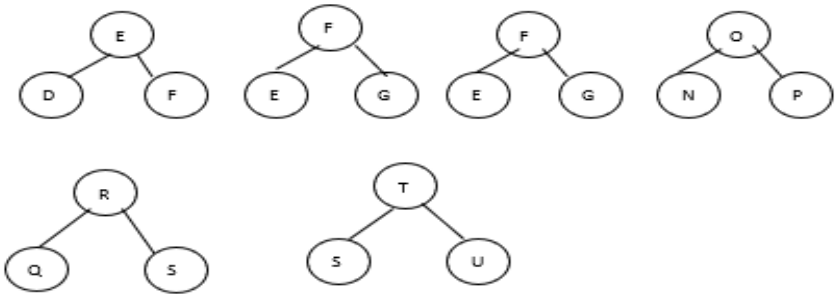
1. Get the Plain text

   EFFORT

2. Append prefix and suffix value to each character in the plain text



3. Form the binary search tree for each character after appending prefix and suffix value



4. Write the intermediate text as per in the binary search tree order

DEFEFGEFGNOPQRSSTU

The Encrypted plain text of **EFFORT : DEFEFGEFGNOPQRSSTU**

4.2 Decryption Process

1. Get the encrypted data.
2. Represent the intermediate text in matrix format using calculations based on the number of characters in the intermediate text. The formula for N intermediate characters M=N/3 then construct 3*M Matrix. Write the intermediate characters in the matrix.

N= 18

M= 18/3 = 6 Hence 3*6 Matrix

α	β	γ	δ	ε	λ
D	E	F	E	F	G
E	F	G	N	O	P
Q	R	S	S	T	U

Let us assume the positions as α,β,γ,δ,ε and λ as Greek letters. And assume the positions α = 1, β=2, γ =3 and so on.

3. Calculation of location,

E(Wi) = η = 2 for i = 1 location = 2 hence M(1, η)

η +3 <= M-1 then Location M(1,η) or M(2, η)

η +3 >= M*2 the location M(2,η)

else η +3 is in the location M(3,η)

First character in the position of E(Wi) = η = 2 for i = 1 location = 2 hence M(1, η) , η = 2 hence β = 2, M(1, β) = E

4. Second character in the position of β +3 = 5 = ε hence M(1, ε) = F
5. Third character is in the position of ε + 3 = β hence M(2, β) = F
6. Fourth character is in the position of β +3 = ε hence M(2, ε) = O
7. Fifth character is in the position of ε + 3 = β hence M(3, β) = R
8. Sixth character is in the position of β +3 = ε hence M(3, ε) = T
9. the number of characters in plain text is equivalent to M Characters

M = 6 hence the original text has 6 characters length.

Original Plain Text = **EFFORT**

5. Results and Discussions

To study the efficiency of thenovel proposedAFR encryption algorithm, it was compared with respect to other encryption such as double encryption and Multiphase encryption algorithms. The proposed encryption algorithm is implemented in PYTHON. The implementation results are shownin the figure 3. The proposed encryption algorithm is analyzed with various ranges of original input data and the corresponding cipher text messages.

Few case studies have been carried out with sampling size varying from 20000 to 100000 bytes of data; the results are shown in the **Table 1** and **Figure. 3** for analyzing the Time efficiency study of the proposed encryption algorithm.

To give more prospective about the performance of the compared algorithms, this section discusses the results obtained from other standard encryption algorithm likes AES,DES, 3DES with proposed algorithm.Their performance is compared by encrypting input files of varying contents and sizes. The algorithms were implemented in a uniform language (Python), using their standard specifications.

Table 1. Results of Case Studies

SNO	Data Samples in bytes	Time taken to encrypt & Decrypt in seconds					
		DES	3DES	AES	Double Encryption [9]	Multiphase Encryption [7]	Proposed Method
1	20000	2.5	6.9	4.3	5.1	6.2	5.8
2	40000	5.2	17.1	8.9	6.8	7.2	9.6
3	60000	6.8	24.2	11.1	7.9	8.2	12.7
4	80000	8.4	27.1	13.4	8.2	8.8	14.6
5	100000	9.6	30.2	15.3	9.5	9.104	16.8

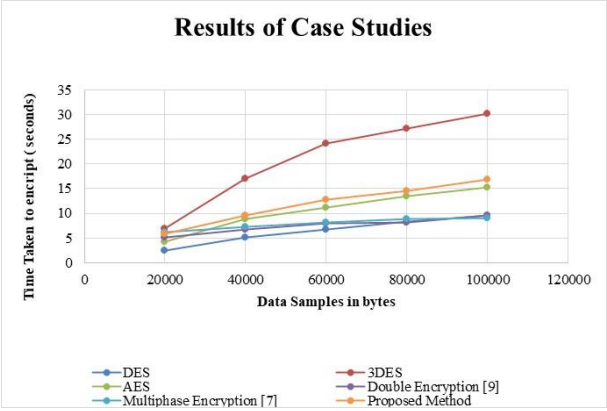


Figure 3 Results ofCase Studies

5.1 Performance Analysis

From the results it is observed that the DES is very good compared to other algorithms. When the sample size increases then Multiphase encryption algorithm performs well. Amazingly it also shows that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data. The Proposed algorithm shows greater performance than 3DES and Multiphase and relative performance to AES.

6. Conclusion

Security plays an important role in modern Cryptography concepts
while transmitting and receiving information. The advantage of this proposed encryption algorithmis that it provides better security in which plain text is modified by appending of prefix and suffix and also representation in the form of BST and which is rewritten as in-order tree traversal manner and produces intermediate results N. Similarlythe decryption process is also made complex which engages the cipher text representation in 3*M matrix format and plain text location identification also requires calculation of η values every time. Hence, it is very difficult to reproduce the original plain text. This study enhances the security in the encryption techniques.

References

[1] S.Suguna,V.Dhanakoti,R.,Manjupriya, A Study on Symmetric and Asymmetric Key Encryption Algorithms, International Research Journal of Engineering and Technology, Vol.3,No. 4, pp. 27 – 31, April,2016.

[2] Gahan.A., V.Geetha., D.Devanagavi , A Empirical Study of Security Issues In Encryption Techniques, International Journal of Applied Engineering Research, Vol.14, No.5, pp. 1049-1061,May, 2019.

[3] Sreyam Dasgupta., Pritish Das, Extended AES Algorithm with Custom Encryption for Government-level Classified Messages, International Journal of Innovative Technology and Exploring Engineering, Vol.8, No.8, pp. 2526 – 2531,August, 2019.

[4] S. Muthusundari, R. M. Suresh, An enhanced D-Shuffle Sorting algorithm for secured encryption message to represent in tree, 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies, Ramnad, Tamil Nadu, 2014, pp. 1583-1588.

[5] S.Muthusundari, A new Divide and Shuffle Based algorithm of Encryption for Text Message, Australian Journal of Basic and Applied Sciences, Vol.9, No.20,pp. 492-496, October, 2015.

[6] Rajni Jain., Ajit Shrivastava, Design and Implementation of New Encryption algorithm to Enhance Performance Parameter, IOSR Journal of Computer Engineering, Vol. 4, No. 5, pp.33-39, April, 2012.

[7] Himanshu Gupta.,Vinod Kumar Sharma, Multiphase Encryption: A New Concept in Modern Cryptography, International Journal of Computer Theory and Engineering, Vol.5, No.4, pp. 638 – 640, April,2013.

[8] Balajee Maram., Lakshmana Rao.K., Ramesh Kumar.Y, Encryption and Decryption Algorithm using 2-D Matrices, International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3,No.4, pp. 352 – 356, April, 2013.

[9] Yashpalsingh Rajput, An Improved Cryptographic Technique to Encrypt Text using Double Encryption, International Journal of Computer Applications, Vol.86, No.6, pp. 24 – 28, June, 2014.

[10] Paresh Ratha et.al, An optimized encryption technique using an arbitrary matrix with probabilistic encryption, Procedia Computer Science Vol.57, pp. 1235 – 1241, July,2015.

[11] Nishtha Mathur, Rajesh Bansode, AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection, Procedia Computer Science,Vol.79,pp. 1036 – 1043,October,2016..

[12] Kalaichelvi V et.al, A New variant of Hill Cipher Algorithm for Data Security, International Journal of Pure and Applied Mathematics, Vol.117, No.15, pp. 581-588, October, 2017.

[13] Swapnil et.al, A Research Paper on New Hybrid Cryptography Algorithm, International Journal for Research & Development in Technology,Vol.9, No.5,May,2018.

[14] S. Sanal Kumar., S. Anfino Sherfin A cryptographic encryption technique byte – Spiral rotation encryption algorithm, Journal of Discrete Mathematical Sciences and Cryptography, Vol.22,No. 3,pp. 371-376,March, 2019.

[15] Syed Tariq Shah Waqif., Ayed Najmuddin Sadaat, Enhance classic Matrix Cryptography using Three-Pass Protocol, Journal of Emerging Technologies and Innovative Research, Vol.7, No.3, pp. 256 – 262, March,2020.

[16] Laia , E M Zamzami and Sutarman, Analysis of Combination Algorithm Data Encryption Standard (DES) and Blum-Blum-Shub (BBS), 5 th International Conference on Computing and Applied Informatics (ICCAI 2020) Journal of Physics: Conference Series 1898 (2021) 012017 IOP Publishing doi:10.1088/1742-6596/1898/1/012017.

[17] Lu, Z.M. and Mohamed, HA Complex Encryption System Design Implemented by AES. Journal of Information Security, Vol.12,No.1,pp. 177-187, January, 2020.