International Journal of Pure and Applied Mathematics
Volume 119 No. 12 2018, 13309-13315
ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

A Hybrid Technique for Enhancing Data Security

G. Manikandan*, P.Harini , K.HariniRajalakshmi
School of Computing, SASTRA Deemed University, Thanjavur, India
*Corresponding Author

Abstract — **The worldwide information and technology has an astounding dependency on data security. The risk fabricated by the interloper has been a maelstrom for forthcoming specialists. Security plays an essential role in governing the data transfer. The primary objective of this paper is to propose a black box approach which generates a modified plain text from the original message. For this purpose, we have used techniques like Perturbation, Swapping and Shifting which will modify the original plain text. Before giving the plain text directly into encryption process, the modified plain text obtained from above techniques will be given as an input. The complexity of breaking the plain text is increased by applying the above techniques. For experimental purpose, we use AES algorithm for encryption and decryption and Java is used for implementing the proposed approach.**

***Index Terms* — AES, Plaintext, Security, Encryption, Decryption**

I.INTRODUCTION

Cryptography is the art of keeping information secure from an unintended audience. Symmetric key algorithm uses the same key for both encryption and decryption. The keys can be identical or it can be different in encryption and decryption.

Symmetric key encryption is the only encryption which was designed before the public key encryption was discovered. Generally, in Symmetric Key cryptography, the algorithm is not kept secret between the sender and the receiver, but the keys are kept secret from others. Sender and Receiver must have the copies of keys that are common to them [1].

Modern cryptographers emphasize that the security not only depends on the secrecy of the encryption method but it can also be achieved using the modified plain text [2]. In cryptography, the plain text is a term that refers to an original message, and the cipher text is the encoded text obtained as a result of the encryption process [18-27].

The aim of a hacker is to retrieve the key and the plain text. In order to increase the security, the original plain text is modified and it is given as an input to AES encryption algorithm. Encryption and decryption process is elaborated in the next section.

II.LITERATURE SURVEY

Six encryption algorithms namely, Blowfish, RC2, RC6, AES, DES and 3DES were evaluated. These algorithms were compared using parameters such as Size of data blocks, Power Consumption, Key size and speed. The authors conclude that Blowfish algorithm had a better performance when compared with the other algorithms. [3-4].

In order to increase the efficiency, the authors have proposed an architecture to perform transformation by integrating Mixcolumn and pre-process InvMixcolumn. From the experimental analysis, it can be inferred that this architecture results in improved security. [5].

In [6], a Hardware implementation of the AES was used for Encryption and Decryption. This approach provides enhanced security and a significant increase in the throughput than the available software models.

The proposed framework consists of four different modules namely Public key-Public key technique, Public key-Private key technique, Private Key-Public key technique and Private Key-Private key technique. From the analysis, it is inferred that Private Key-Private key technique is the more appropriate one for transmitting confidential data in a secured manner. This technique also ensures confidentiality and availability among the communicating parties. The limitation of this framework is that it supports limited users. [7-8]

The use of Turing-machine to generate the equivalent binary number for a given decimal number is proposed. The authors used this approach to find the next successor of the given decimal number. This approach can be used in cryptography to enhance the data security. [9]

Two symmetric cryptographic algorithms namely AES and Blowfish are used to enhance data security. S-box columns of AES are modified and used with Blowfish to increase confidentiality. To measure the performance of the proposed approach, encryption and decryption are done with different file types. [10]

A hybrid model integrating AES and DES was proposed for security enhancement [11-13]. This model provides better non-linearity than the original AES. As a result of more number of computations, the time taken for encryption

and decryption in this model is more than its individual counterparts [28-36].

Cryptography and Steganography are combined to achieve data security enhancement [14-16]. The original message is converted into cipher text using a cryptographic algorithm and the resultant cipher text is embedded in an image [37-42]. The stego image is sent to the receiver over a public network. It is also proved that the PSNR value lies within the acceptable level for various data payload sizes.

The authors have proposed a system using transposition technique to increase the security of DES algorithm. Various transposition techniques available in the literature are as follows: Rail Fence Technique, Simple Columnar Transposition Technique, Vernam Cipher (One-Time Pad) and Book Cipher/Running Key Cipher. In this work, Simple Columnar Transposition Technique with Multiple Rounds (SCTTMR) was used. The original plain text is modified by using the proposed

Simple Columnar Transposition Technique is used to generate the cipher text in the first round. The same technique is repeated for multiple rounds to increase the security. The cipher text generated at the end of multiple rounds is given as input to the DES algorithm. The main disadvantage of this scheme is time consumption. The time taken by the proposed approach is directly proportional to the number of rounds [17].

III.PROPOSED SYSTEM

The security in data transmission is improved by using proposed techniques. Initially, the plain text is obtained from the user and then it is modified using three main techniques, that techniques are Perturbation, Swapping, and Shifting. The Fig. 1 represents the proposed system in the form of a block diagram and the Fig. 2 is an example to illustrate our proposed system in the form of a block diagram.

Perturbation is the process of adding noise to the given plain text. The given plain text which contains alphabets and numbers can be converted to its corresponding alphabets and numbers depending upon the noise specified. First, the given plain text is cleaved into two chunks, and then the noise will be added in each and every odd positions in both the chunks. Then, the data chunks are given to the swapping technique.

In swapping, the two chunks from the perturbation is taken as an input. First of all, each chunk will be split into two parts. The first part and the last part will be swapped such that the first part gets placed in the last and the last part gets placed in the first and then the output from each chunk will be given as an input to the Shifting process.

In the shifting process, input from swapping process is split into two parts, and then the alphabet or the number gets swapped with the next alphabet or the number that is present next to it. Finally, the data chunks are merged together. This final data chunk is the modified plain text which will be given as an input to the encryption algorithm.

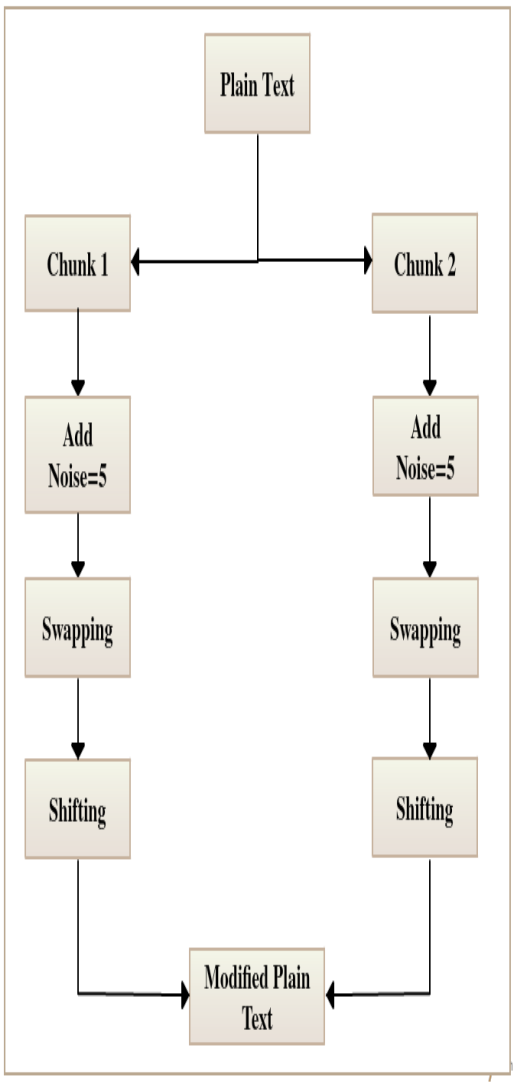

Fig. 1. Flow diagram of Proposed System

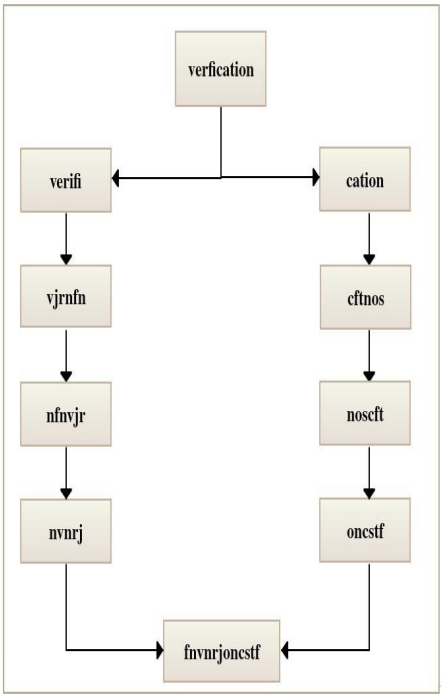

Fig. 2. Flow diagram of Proposed System with an Example

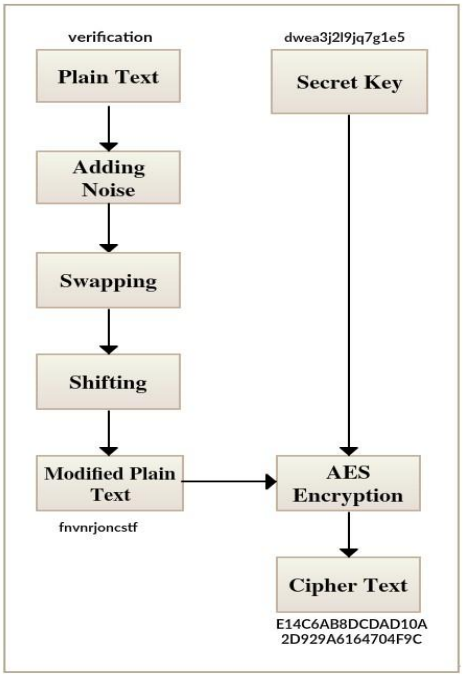

Fig. 3. Flow diagram of Encryption process

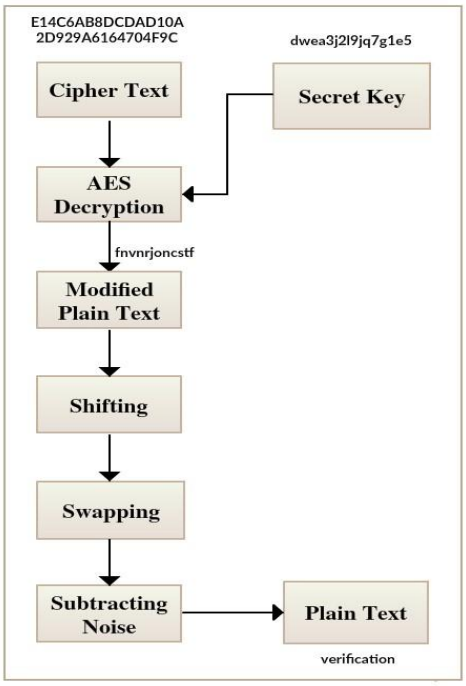

Fig. 4. Flow diagram of decryption process

After successful processing of Perturbation, Swapping and Shifting, the modified plaintext is loaded as input to the Encryption Phase. The key size of 16, 24 or 32 entered. The input modules get processed and the encrypted cipher text is generated. The modified cipher text is provided as input to the Decryption algorithm. The decrypted modified plain text is inserted to the three main processes as Shifting, Swapping and Perturbation with the subtraction of noise. After performing the above three processes, the original plaintext is obtained. The Fig. 5 and 6 represent Encryption and decryption process which generates the modified plaintext by using proposed techniques

```
G:\Project\CODE>javac Encode.java

G:\Project\CODE>java Encode
Enter the Plain Text
verification
After adding noise                  : vjrnfncftnos
After Swapping                      : nfnvjrnoscft
After Shifting Modified Plain Text is : fnvnrjoncstf
G:\Project\CODE>
```

Fig. 5. Snapshot representing Encryption Result

```
G:\Project\CODE>javac Decode.java

G:\Project\CODE>java Decode
Enter the Modified Plain Text
fnvnrjoncstf
After Shifting                              : nfnvjrnoscft
After Swapping                              : vjrnfncftnos
Original Plain Text after subtracting noise : verification
G:\Project\CODE>
```

Fig. 6. Snapshot representing Decryption Result

IV. EXPERIMENTAL ANALYSIS

The proposed methodology determines the modified plain- text to be fed as input to the Encryption phase which uses AES algorithm as the process. The cipher text obtained is decrypted and proceeds with the shifting, swapping and subtraction of noise and ends with the extraction of plain text. The proposed outlook is executed using Java programming language and the outcome is tested using a Corei3 processor with 4GB RAM with Windows 8 operating system. By the exploratory results, the encryption and decryption process with modified plain text involving Perturbation, shifting and swapping methods will provide foremost results for effective data transmission and advancement in data security.

V.SECURITY ANALYSIS

The aim of the attacker is to find the secret key and plaintext from the cipher text. In order to complicate the job of the attacker, we need to increase the complexity of the algorithm. To test the complexity, the analysis is done in following attacks.

1) Brute force attack
2) Known plaintext attack
3) Chosen plaintext attack
4) Chosen cipher text attack

In Brute force attack, the complexity of key is tested. Based on the key size complexity is increased, AES algorithm is implemented in this approach, which has minimum key size 128 bits and the maximum key size of 256 bits. Hence the size of the key space is

$$2^{256} = (2^{10})^{25.6} \approx (10^{3})^{25.6} = 10^{76} \quad (1)$$

The time required to find the plaintext with one key value in the key space is 10^{-7} seconds and the time required for the execution of the cipher with all the possible keys in the keyspace is

$$\frac{10^{76} \times 10^{-7}}{365 \times 24 \times 60 \times 60} = 3.17 \times 10^{61} \quad (2)$$

As the number of possible keys is too large, it is impractical to break the ciphertext. The relation between the plaintext and the cipher text is

C=Noise (Swap (Shift (AES algorithm relation))) (3)

It makes it impossible for the chosen plaintext attack or chosen cipher text attack to break the cipher text. In the light of the above discussion of cryptanalysis, we finally conclude that this cipher is a strong one, and it cannot be broken by any easy means.

VI.CONCLUSION

This paper introduces a modern approach for enhancement of data security. The novelty of the system is that the original plain text is divided into many chunks and each chunk will undergo perturbation, swapping and shifting in the same sequence.The modified plain text is inserted as input to the Encryption algorithm.AES Encryption and Decryption algorithms are used for desirable security of plain text. The encrypted cipher text is introduced into Decryption algorithm to obtain the modified plain text. Similarly, the modified plaintext is converted into plain text by subtraction of noise, swapping and shifting. In the upcoming work, the security level of key generation can be increased by adding digital signature methodology

ACKNOWLEDGMENT

The authors would like to thank the Department of Science and Technology, India for their financial support through Fund for Improvement of S&T Infrastructure (FIST) programme SR/FST/ETI-349/2013.

REFERENCES

1. William Stallings. Cryptography and Network Security. Wiley; 1995.

2. Bruce Schiner. Applied Cryptography. John Wiley; 1996.

[3] Sachin Sharma , Jeevan Singh Bisht , "Performance Analysis of Data Encryption Algorithms" International Journal of Scientific Research in Network Security and Communication , 3(1) , 2015 , 1-5.

[4] G.Manikandan, R.Manikandan, G.Sundarganesh. A New Approach for Generating Strong Key in RC4 Algorithm. Journal of Theoretical and applied information Technology. 2011. 24; pp.113-119.

[5] Yu-Jung Huang, Yang-Shih Lin, Kuang-Yu Hung,Kuo-Chen Lin 2006 "Efficient Implementation of AES IP", IEEE Asia Pacific Conference on Circuits and Systems, 2006

[6] Subashri T, Aruna chalam R, Gokul Vinoth Kumar B ,Vaidehi V, "Pipelining Architecture of AES Encryption and Key Generation with Search Based Memory" , International Conference on Network Security and Applications. CNSA 2010. Communications in Computer and Information Science, vol 89. 224-231

[7]Natasha Saini ,Nitin Pandey, Ajeet Pal Singh ENHANCEMENT OF SECURITY USING CRYPTOGRAPHIC TECHNIQUES , 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 2015

[8] G.Manikandan, R. DalhousePrabu, P. SravanKumar, M. SudhakarRaj, S. Venkatakrishnan. Rendering A Fortify Key to Enhance the Security of Cryptographic Algorithms. International Journal of Applied Engineering Research. 2014. 9; pp.1987-1955.

[9] Himanshu Tripathi, Bramah Hazela Data Security Enhancement Through Number System 2016 Second International Conference on Computational Intelligence & Communication Technology,632-637

[10] Shaikh Ammarah P, Vikas Kaul and S K Narayankhedkar Security Enhancement Algorithm for Data Transmission using Elliptic Curve Diffie - Hellman Key Exchange, International Conference & workshop on Advanced Computing 2014 (ICWAC 2014) – 10-16

[11] Jigar Chauhan , Neekhil Dedhia , Bhagyashri Kulkarni Enhancing Data Security by using Hybrid Cryptographic Algorithm International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 3, May 2013 221-228.

[12] S.Karthikeyan, N.Sairam, G.Manikandan, J.Sivaguru. A Parallel Approach for Improving Data Security. Journal of Theoretical and Applied Information Technology. 2012. 39; pp. 119-125.

[13] S.Karthikeyan, N.Sairam, G.Manikandan. A New Approach for Enhancing Data Security Using Parallel Processing. Advances in Natural and Applied Sciences. 2012. 6; pp.696-703.

[14] T. M. Sadikot, Dr. D. G. Kamdar Data Security Enhancement with Crystography – A Combination of Cryptography and Steganography International Journal Of Darshan Institute On Engineering Research & Emerging Technologies Vol. 4, No. 1, 2015 , 1-6.

[15] G.Manikandan, P.Rajendiran, K.Chakarapani, G.Krishnan, G.SundarGanesh. A Modified Crypto Scheme for Enhancing Data Security. Journal of Theoretical and applied information Technology. 2012. 35; pp.149-154.

[16] G.Manikandan, N.Sairam, M.Kamarasan. A Hybrid Approach for Security Enhancement by Compressed Crypto-Stegno Scheme. Journal of Applied Sciences, Engineering and Technology. 2012. 4; pp.608-614.

[17] Sombir Singh, Sunil K. Maakar Dr.Sudesh Kumar, Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, vol 3(6), 2013 , pp. 464-471.

[18] Logesh, R., Subramaniyaswamy, V., Vijayakumar, V., Gao, X. Z., & Indragandhi, V. (2017). A hybrid quantum-induced swarm intelligence clustering for the urban trip recommendation in smart city. Future Generation Computer Systems, 83, 653-673.

[19] Subramaniyaswamy, V., & Logesh, R. (2017). Adaptive KNN based Recommender System through Mining of User Preferences. Wireless Personal Communications, 97(2), 2229-2247.

[20] Logesh, R., & Subramaniyaswamy, V. (2017). A Reliable Point of Interest Recommendation based on Trust Relevancy between Users. Wireless Personal Communications, 97(2), 2751-2780.

[21] Logesh, R., & Subramaniyaswamy, V. (2017). Learning Recency and Inferring Associations in Location Based Social Network for Emotion Induced Point-of-Interest Recommendation. Journal of Information Science & Engineering, 33(6), 1629–1647.

[22] Subramaniyaswamy, V., Logesh, R., Abejith, M., Umasankar, S., & Umamakeswari, A. (2017). Sentiment Analysis of Tweets for Estimating Criticality and Security of Events. Journal of Organizational and End User Computing (JOEUC), 29(4), 51-71.

[23] Indragandhi, V., Logesh, R., Subramaniyaswamy, V., Vijayakumar, V., Siarry, P., & Uden, L. (2018). Multi-objective optimization and energy management in renewable based AC/DC microgrid. Computers & Electrical Engineering.

[24] Subramaniyaswamy, V., Manogaran, G., Logesh, R., Vijayakumar, V., Chilamkurti, N., Malathi, D., & Senthilselvan, N. (2018). An ontology-driven personalized food recommendation in IoT-based healthcare system. The Journal of Supercomputing, 1-33.

[25] Arunkumar, S., Subramaniyaswamy, V., & Logesh, R. (2018). Hybrid Transform based Adaptive Steganography Scheme using Support Vector Machine for Cloud Storage. Cluster Computing.

[26] Indragandhi, V., Subramaniyaswamy, V., & Logesh, R. (2017). Resources, configurations, and soft computing techniques for power management and control of PV/wind hybrid system. Renewable and Sustainable Energy Reviews, 69, 129-143.

[27] Ravi, L., & Vairavasundaram, S. (2016). A collaborative location based travel recommendation system through enhanced rating prediction for the group of users. Computational intelligence and neuroscience, 2016, Article ID: 1291358.

[28] Logesh, R., Subramaniyaswamy, V., Malathi, D., Senthilselvan, N., Sasikumar, A., & Saravanan, P. (2017). Dynamic particle swarm optimization for personalized recommender system based on electroencephalography feedback. Biomedical Research, 28(13), 5646-5650.

[29] Arunkumar, S., Subramaniyaswamy, V., Karthikeyan, B., Saravanan, P., & Logesh, R. (2018). Meta-data based secret image sharing application for different sized biomedical images. Biomedical Research,29.

[30] Vairavasundaram, S., Varadharajan, V., Vairavasundaram, I., & Ravi, L. (2015). Data mining ‐ based tag recommendation system: an overview. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 5(3), 87-112.

[31] Logesh, R., Subramaniyaswamy, V., & Vijayakumar, V. (2018). A personalised travel recommender system utilising social network profile and accurate GPS data. Electronic Government, an International Journal, 14(1), 90-113.

[32] Vijayakumar, V., Subramaniyaswamy, V., Logesh, R., & Sivapathi, A. (2018). Effective Knowledge Based Recommeder System for Tailored Multiple Point of Interest Recommendation. International Journal of Web Portals.

[33] Subramaniyaswamy, V., Logesh, R., & Indragandhi, V. (2018). Intelligent sports commentary recommendation system for individual cricket players. International Journal of Advanced Intelligence Paradigms, 10(1-2), 103-117.

[34] Indragandhi, V., Subramaniyaswamy, V., & Logesh, R. (2017). Topological review and analysis of DC-DC boost converters. Journal of Engineering Science and Technology, 12 (6), 1541–1567.

[35] Saravanan, P., Arunkumar, S., Subramaniyaswamy, V., & Logesh, R. (2017). Enhanced web caching using bloom filter for local area networks. International Journal of Mechanical Engineering and Technology, 8(8), 211-217.

[36] Arunkumar, S., Subramaniyaswamy, V., Devika, R., & Logesh, R. (2017). Generating visually meaningful encrypted image using image splitting technique. International Journal of Mechanical Engineering and Technology, 8(8), 361–368.

[37] Subramaniyaswamy, V., Logesh, R., Chandrashekhar, M., Challa, A., & Vijayakumar, V. (2017). A personalised movie recommendation system based on collaborative filtering. International Journal of High Performance Computing and Networking, 10(1-2), 54-63.

[38] Senthilselvan, N., Udaya Sree, N., Medini, T., Subhakari Mounika, G., Subramaniyaswamy, V., Sivaramakrishnan, N., & Logesh, R. (2017). Keyword-aware recommender system based on user demographic attributes. International Journal of Mechanical Engineering and Technology, 8(8), 1466-1476.

[39] Subramaniyaswamy, V., Logesh, R., Vijayakumar, V., & Indragandhi, V. (2015). Automated Message Filtering System in Online Social Network. Procedia Computer Science, 50, 466-475.

[40] Subramaniyaswamy, V., Vijayakumar, V., Logesh, R., & Indragandhi, V. (2015). Unstructured data analysis on big data using map reduce. Procedia Computer Science, 50, 456-465.

[41] Subramaniyaswamy, V., Vijayakumar, V., Logesh, R., & Indragandhi, V. (2015). Intelligent travel recommendation system by mining attributes from community contributed photos. Procedia Computer Science, 50, 447-455.

[42] Vairavasundaram, S., & Logesh, R. (2017). Applying Semantic Relations for Automatic Topic Ontology Construction. Developments and Trends in Intelligent Technologies and Smart Systems, 48.