DOI: http://dx.doi.org/10.26483/ijarcs.v9i1.5285

Volume 9, No. 1, January-February 2018

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

AN ENHANCED ADVANCED ENCRYPTION STANDARD (EAES) ALGORITHM FOR SECURE FIBER OPTIC COMMUNICATION

Bosco Paul Alapatt,
Research Scholar,
Department of Computer Science,
Bharathiar University, Coimbatore, India

Dr. A. Kavitha
Assistant Professor
Department of Computer Science,
Kongunadu Arts and Science College, Coimbatore, India

***Abstract*:** Fiber optic communication is a part of optical communication where the data is transmitted and received via optical cables. It is widely used due to its advantages over traditional communication systems. Security is considered as a main concern in any communication systems. Since fiber optics transfers data efficiently for longer distances, an end to end secured fiber optic communication is very difficult. Advanced encryption Standard (AES) is a symmetrical encryption algorithm which founds to be more secure, faster and stronger where tapping of data is not quite easy. As the cyber attacks are continuously developing, AES algorithm is broken by some attacks namely brute force, differential, algebraic and linear attacks. To overcome the limitations of AES algorithm, a new enhanced AES algorithm abbreviated as EAES algorithm is proposed for secured fiber optic communication. EAES differs from AES algorithm in two ways: Dynamic Key Generation and Dynamic s-box generation. It increases the complexity to break the encryption process and also makes it more difficult for the attacker to hack the data. The proposed EAES algorithm is simulated and the results are analyzed in terms of throughput and conversion time. The results show that the EAES method attains higher end to end security in fiber optic communication.

***Keywords*:** AES algorithm, cyber attacks, encryption, fiber optic communication

1. INTRODUCTION

Fiber optic communication is a part of optical communication and is used in situations where high speed data transmission over long distances is needed. It transmits data using the fiber optic cable based on the principle of total internal reflection. It became very popular due to its advantages such as less delay, high data rate, fast uploading, long distance communication and so on [1]. It is useful from commercial to military applications. It transmits different types of data like text, images, audios, videos, etc. it is very beneficial than traditional communication such as lesser attenuation, lower bandwidth, lesser weight and null interference [2]. Though the full bandwidth is not utilized, still it transmits data at a rate of gigabits per second. Fiber optic cable communicates data over a distance of 100 kilometers and the copper wire sends data to a minimum distance of 2 kilometers.

The block diagram of the fiber optic communication is shown in Fig. 1. The major blocks are transmitter, fiber optic cable, receiver and a regenerator. The transmitter transforms the input data to optical signals and transmitted via a light source. The light source can be a laser or Light Emitting Diode (LED). The optical signals are passed to the fiber optic cable and reach the receiver. The receiver contains a photo detector which converts back the received light signal to electrical signals. During the long distance communication, a regenerator is needed to increase or boost light signals.

Despite of various advantages of fiber optic communication, it is easily vulnerable to various types of attacks. The data transmitted via copper cables is highly insecure when compared to fiber optic communication. In some situations, the attacker accesses to the fiber cable and easily taps the data [3]. When the attacker utilizes a laptop, customized software, optical tap and an opto-electronic converter, then the attack will be not be easily identified. This customized software behaves as a filter and it allows access to particular IP address, Mac address and relevant sensitive information [4],[5]. With no disturbance to the actual data transmission, the attacker can tap the data in a simple way.

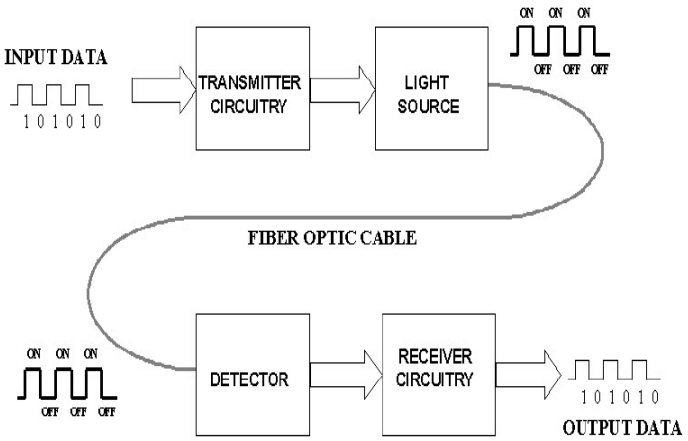

Fig. 1. Block diagram of fiber optic communication

1.1 Contribution of this paper

This paper presents an enhanced AES (EAES) algorithm for secured fiber optic communication. It improves the performance of AES algorithm and makes is more secure by the inclusion of two process: Dynamic Key Generation and Dynamic s-box generation. It increases the complexity to break the encryption process and also makes it more difficult for the attacker. The proposed EAES algorithm is simulated and the results are analyzed in terms of throughput and conversion time. The results show that the

EAES method attains higher end to end security in fiber optic communication.

1.2 Organization of this paper

The residue of the paper is structured as follows. The existing encryption algorithms and the demerits of AES algorithm is discussed in Section 2. The EAES algorithm is described in Section 3. Section 4 provides the performance evaluation and the paper is ended in Section 5.

2. RELATED WORK

Nowadays, cyber attacks are rapidly increasing and it is hard to safeguard end to end data transmission. Encryption is the only way to prevent data from the attacker. Encryption is the process of transforming the input plain text to cipher text with the help of some underlying process. The selection of key is highly important which affects the overall performance of any encryption process. Secrecy and Length of the key are significant factors of an encryption key. The key can be numerals or alphabets or alpha-numerals or special symbols [6].

AES is an efficient algorithm to achieve security in data transmission. Singh et al. [7] preformed a study on 3 encryption algorithms namely RSA, DES and Triple DES and AES to identify their performance on the basis of speed, time, and throughput and avalanche effect. The results shows that AES is found to more secure than other compared algorithms. Another study is conducted in [8] to compare AES, DES and RSA algorithm. The performance analysis indicates that AES encrypts the data at a faster rate than RDA and DES. In addition, decryption of AES algorithm is better than other algorithms. Padmavathi et al. [9] developed 3 encryption algorithms like DES, RSA and AES with Least Significant Bit Substitution to investigate the efficiency of encryption and decryption time. [10] employed Dynamic key generation in AES to handle vulnerabilities. Here, the key is created randomly using the time of the transmitter. In the decryption side, a time value is used with some tolerance limits to identify the similar key pair of the time value created in the encryption process. It is found to be stronger than traditional AES algorithm.

Janadi et al. [11] presented a dynamic S-box approach to maximize the immunity level of AES algorithm to prevent algebraic attacks. The introduction of dynamic substitute-box makes it more complex to break down. Sahmoud et al. [12] developed a method which uses various sub-keys from the original key and each sub-key is employed in every round. The usage of more number of sub-keys in the encryption process prevents the brute force attack.

The main demerits of the AES algorithm are:

- The increasing number of Cyber-attacks faces a threat to break AES algorithm
- Symmetric algorithm are easily breakable by Brute-force Attack, Differential Attack, Algebraic Attack and Linear Attack [13][14][15].
- When a symmetric algorithm is broken, then more loss will be occurred.

To overcome the above-mentioned drawbacks, enhanced AES (EAES) algorithm for secured fiber optic communication is proposed. It increases the security level by the use of dynamic key generation and dynamic S-box generation.

3. ENHANCED ADVANCED ENCRYPTION STANDARD

Encryption algorithms are mandatory to provide secure data transmission over fiber optic communications. The optic transmitter encrypts the message using the proposed EAES algorithm and generates the cipher text. The cipher text will be transmitted from optic transmitter to optic receiver via fiber optic cable. The optical receiver receives the cipher text and executes the decryption algorithm. The decryption process is the exact reverse process of encryption process. The optical receiver recovers the original message from the cipher text. Thus, EAES algorithm achieves end to end secured fiber optic communication. The overall operation of the EAES algorithm is shown in Fig. 2.

AES involves 4 stages including one permutation and three substitution stages. The overall operation of AES algorithm is shown in Figure. 4.

• **Substitute Byte**: Every individual byte in matrix is altered by 8-bit substitution box i.e. S-box.
• **ShiftRows**: It is a transposition step in which the last three rows of the state are shifted cyclically a particular number of steps. 1st row is kept unchanged, 2nd row rotated by 1st row, 3rd row is rotated by 2nd row and 4th row is rotated by 3rd row.
• **MixColumns**: Each column of input matrix is multiplied by the mix Column matrix which results to the equivalent column of output matrix.
• **AddRoundKey**: Round key is combined with the state. In every round, a sub key is obtained from the main key using the key scheduling. The round key is appended by combining every byte of state with equivalent byte of round key by bitwise XOR.

The proposed method works on the idea of dynamic key and s-box generation. By increasing the confusion and diffusion in the cipher text by the use of dynamic key generation process, the complexity of the data is gradually increased. Then, Dynamic S-Box Generation makes it hard to break and also difficult to perform any ground work of static set of S-box. It consists of two main phases:

- Dynamic key generation
- Dynamic s-box generation

A. Dynamic Key Generation

AES algorithm uses the function of time to generate the dynamic key. The key is created randomly using the time when the transmitter enters to the system. In the decryption process, the synchronization activity takes time value with a particular tolerance level to identify the similar key pair of the time value obtained in the encryption process. The transmitter in the fiber optic communication system initially generates the dynamic key using the time function. The value of the time of start (VTS) and value of salt (VS) is used to compute the dynamic key.

$$Key=VTS+VS \quad (1)$$

The generated key is used to encrypt the plain text. The key is given as input to the AES encryption algorithm. The dynamic key is given to all rounds and the dynamic s-box is generated consequently.

B. Dynamic S-Box Generation

The Static s-box is converted to dynamic S-box by the use of cipher key. The inverse S-box is also be modified in the EAES algorithm. This is used to make the algorithm stronger. XOR process of all the bytes of cipher key is taken. The resultant Hex value will be used to rotate S-box. The static s-box is converted to dynamic s-box using the cipher key to generate the cipher text. The inverse substitute-box will also be modified in the EAES algorithm. This is done to make AES cryptographically strong. XOR operation of all bytes of cipher key is taken. The resultant Hex value will be employed to rotate S-box. The proposed system introduced confusion in AES algorithm makes it more complex.

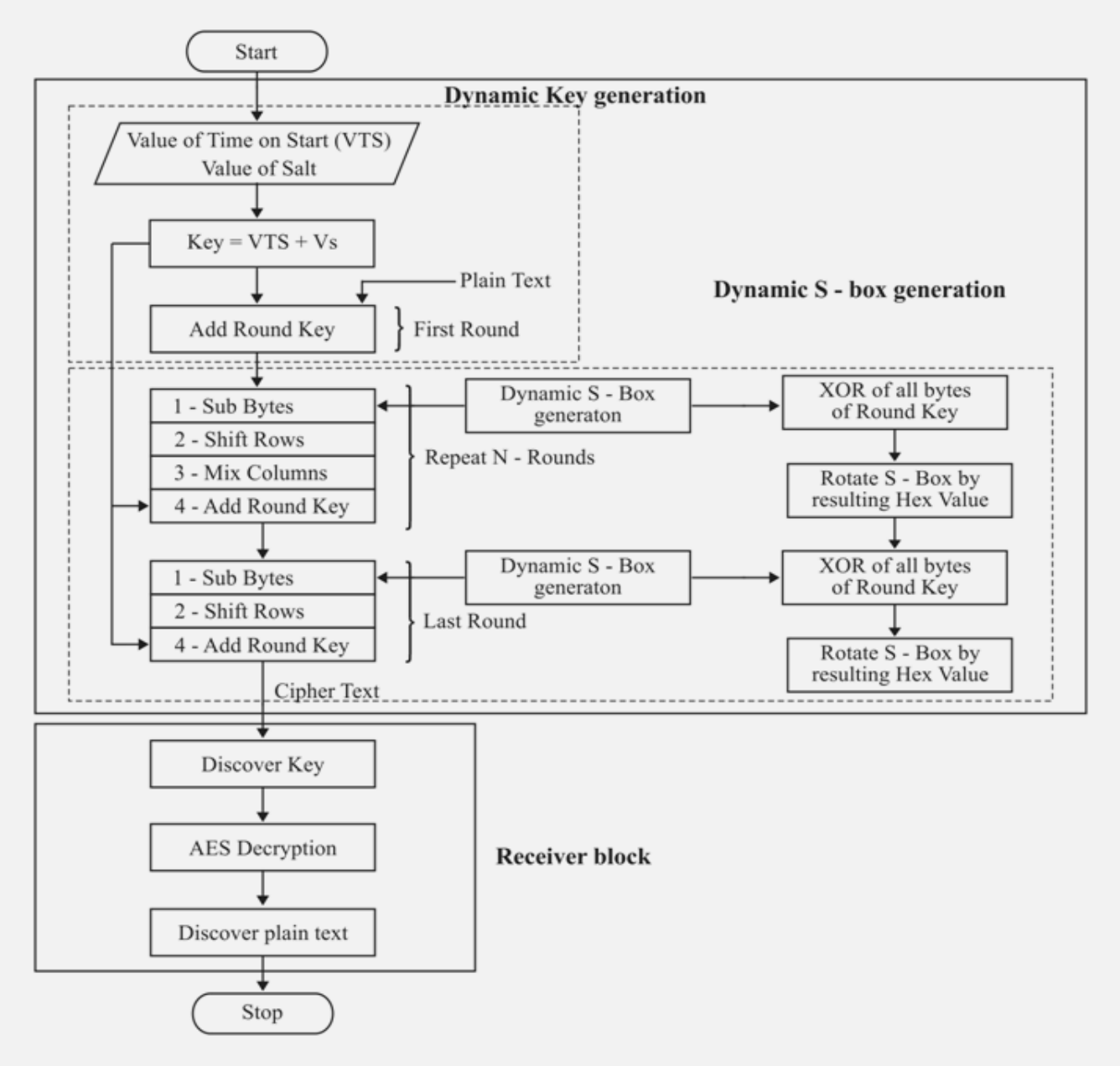

Fig. 2. Work flow of EAES algorithm in fiber optic communication

4. EXPERIMENTAL ANALYSIS

This section presents the performance metrics used to analyze the performance of the EAES algorithm. This method is implemented in a PC Intel core i3, 170GHz processor with 4GB RAM.

4.1 Metrics

The parameters used to investigate the performance of the EAES algorithm are mentioned below.

- Encryption time
- Decryption time

- Throughput

- **Encryption time:** Encryption time is the time taken to generate the cipher text from the plain text and is measured in seconds. It indicates the actual speed of the encryption process.
- **Decryption time:** Decryption time is the time taken to recover the plain text from the cipher text and is measured in seconds. It indicates the actual speed of the decryption process.
- **Throughput:** The throughput is defined as the ratio of the amount of plain text in bytes encrypted to the encryption time.

4.2 Results and Discussion

The effectiveness of EAES algorithm is investigated by the means of conversion time and throughput. The results of conversion time and throughput for several file conversions are shown in Figure 3 and Figure 4 respectively. The results are analyzed based on the conversion time of some files and are listed below.

- Binary to Text and Text to Binary,
- Image to Binary and Binary to Image and
- Number to binary and Binary to Number

4.2.1 Binary to Text and Text to Binary

In the beginning, 36kB text file is used to evaluate the performance of the encryption algorithm. Parameters like throughput and conversion time are calculated. The conversion time and throughput are tabulated in Table 1. The EAES algorithm transforms the text file to binary in 0.006 seconds and converts the binary file to text file in 0.012 seconds. It is noted that EAES algorithm achieves the throughput of 3.8 Mbps for transforming text to binary and 6.56 Mbps while converting binary to text.

Table 1: Conversion of binary to text and text to binary

	Text to binary	**Binary to text**
Conversion time (seconds)	0.006	0.012
Throughput (Mbps)	3.8	6.56

Table 2: Conversion of Image to Binary and Binary to Image

	Image to Binary	**Binary to Image**
Conversion time (seconds)	0.132	0.129
Throughput (Mbps)	5.8	6.56

4.2.2 Image to Binary and Binary to Image

Here, 12kB image file is used to analyze the performance of the EAES algorithm. Parameters like throughput and conversion time are computed. The obtained results of conversion time and throughput are tabulated in Table 2. The proposed method transforms the image file to binary in 0.132 seconds and transforms the binary file to image file in 0.132 seconds respectively. It is also observed that the EAES algorithm achieves the throughput of 5.8 Mbps for converting image to binary and 6.56 Mbps while converting binary to image.

4.2.3 Number to binary and Binary to Number

Here, 36kB number file is employed to compute the performance of the EAES algorithm. Parameters like throughput and conversion time are calculated. The obtained results of conversion time and throughput are tabulated in Table 3. The EAES algorithm translates the number file to binary in 0.012 seconds and again transforms the binary file to number file in 0.018 seconds respectively. It is noted that EAES algorithm attains the throughput of 6.72 Mbps for converting number to binary and 9.72 Mbps for the conversion of binary to number file.

Table 3: Conversion of Number to binary and Binary to Number

	Number to Binary	**Binary to Number**
Conversion time (seconds)	0.012	0.18
Throughput (Mbps)	6.72	9.72

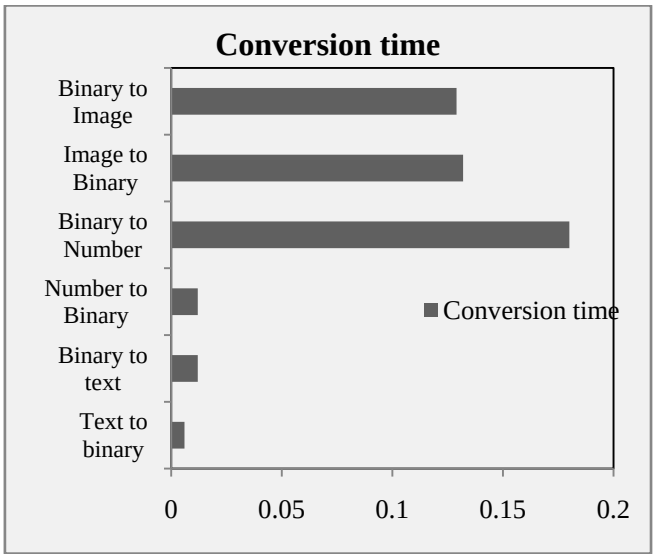

Fig. 3. Conversion time for various file conversions

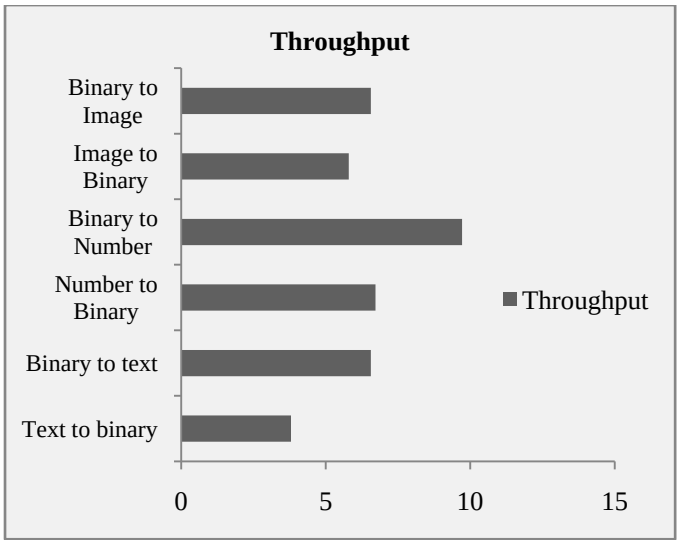

Fig. 4. Throughput for various file conversion

4. CONCLUSION

Security is considered as a main concern in any communication systems. Since fiber optics efficiently transfers data for longer distances, an end to end secured fiber optic communication is very difficult. This paper presents an enhanced AES (EAES) algorithm for secured communication. The EAES algorithm with dynamic key and s-box generation makes the data transmission more secure by adding more complexity in AES by increasing the Confusion and Diffusion in Cipher text. It will safeguard the data from various attacks like brute-force Attack, differential Attack, Algebraic Attack and Linear Attack. It will increase the security level in the end to end fiber optic communication system.

5. REFERENCES

[1] D.C. Agarwal , "Fiber Optic Communication", second edition, 1993

[2] M. Medard, et al., Security issues in all-optical networks, IEEE Netw. 11 (3) (1997) 42–48.

[3] K. Shaneman, S. Gray, Optical network security: technical analysis of fiber tapping mechanisms and methods for detection and prevention, in Military Communications Conference, Monterey, CA, Vol. 2, 2004, pp. 711–716.

[4] The Clip-On Coupler FOD 5503 product specifications, http://www.fods.com/optic_ clip_on_coupler.html (last accessed July 2017).

[5] B. Wu, B.J. Shasti, P.R. Prucnal, Secure communication in fiber-optic networks, in: Emerging Trends in ICT Security, Elsevier, 2014.

[6] P. S. Mukesh, M. S. Pandya and S. Pathak, "Enhancing AES algorithm with arithmetic coding," 2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), pp.83-86, IEEE, 2013.

[7] G. Singh and Supriya, "A study of encryption algorithms (RSA, DES,3DES and AES) for information security," International Journal ofComputer Applications, vol.67, pp. 33-38, April 2013.

[8] P. Mahajan and A. Sachdeva, "A study of Encryption algorithms AES, DES and RSA for security," Global Journal of Computer Science andTechnology, vol.13, pp. 14-22, 2013.

[9] B. Padmavathi and S. R. Kumari, "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution," International Journal of Science and Research (IJSR), vol.2, pp. 170-174, April 2013.

[10] Z. Musliyana, T. Y. Arif and R. Munadi, "Security Enhancement of Advanced Encryption Standard (AES) using Time-Based Dynamic Key Generation," ARPN Journal of Engineering and Applied Sciences,vol.10, pp. 8347-8350 , October 2015.

[11] Janadi and D. A. Tarah, "AES immunity Enhancement against algebraic attacks by using dynamic S-Boxes," 3rd International Conference on Information and Communication Technologies: FromTheory to Applications (ICTTA), pp. 1-6, IEEE, 2008.

[12] S. Sahmoud, W. Elmasry and S. Abudalfa, "Enhancement the Security of AES Against Modern Attacks by Using Variable Key Block Cipher," International Arab Journal of e-Technology, vol.3, pp. 17-26, January 2013.

[13] H. Alanazi, B. B. Zaidan, A.A. Zaidan, H.A. Jalab, M. Shabbir and Y. AI-Nabhani, "New comparative study between DES, 3DES and AES within nine factors," Journal of Computing, vol. 2, pp. 152-157, March 2010.

[14] A. Alabaichi and A. I. Salih, "Enhance security of advance encryption standard algorithm based on key-dependent S-box," 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC), pp. 44-53, IEEE, 2015.

[15] K. Lala, A. Kumar and A. Kumar, "Enhanced throughput AES encryption," IJECSE, vol. 1, p. 2132-2137, 2012.