Security Enhancement of AES-CBC and Its Performance Evaluation Using The Avalanche Effect

Hayder T. Assafli
Department of Electrical Engineering
University of Technology
Baghdad, Iraq
140030@uotechnology.edu.iq

Ivan A. Hashim
Department of Electrical Engineering
University of Technology
Baghdad, Iraq
30095@uotechnology.edu.iq

2020 3rd International Conference on Engineering Technology and its Applications (IICETA) | 978-1-7281-8231-5/20/$31.00 ©2020 IEEE | DOI: 10.1109/IICETA50496.2020.9318803

***Abstract*—The security of communication systems is becoming a significant concern with the increase in computational power. High-security cryptographic algorithms are required to protect the privacy of information from unauthorized access. This paper presents a security enhancement of Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode and its performance evaluation using the Avalanche Effect. In this study, a new improved technique for increasing the security of the AES-CBC is introduced. The Unix time is used as a source for Initialization Vector (IV) in CBC mode before encryption rounds. The results showed that the algorithm generates different ciphertext at each execution. In other words, different ciphertext output significantly decreases the risk of cracking the encryption key. Moreover, the results are examined using the Avalanche Effect and tested for satisfying the security criteria. The achieved results showed that the encryption method succeeds in maintaining the avalanche effect requirement and introducing additional strength to the encryption process by preventing the encryption key update for every new ciphertext.**

Keywords—encryption, Avalanche Effect, Advanced Encryption Standard (AES), Initialization Vector (IV), Continuous Block Chaining (CBC).

I. INTRODUCTION

The development of fast and new computing techniques increased security threats against the block cipher cryptography algorithms. Therefore, higher security devices and systems are required to protect transmitted data through communication systems. So, new cryptographic algorithms are being designed, and different data encryption methods are being developed to protect sensitive information from unauthorized users [1]. The basic idea behind encryption is to convert readable messages into scrambled and encrypted messages that cannot be interpreted by hackers and unwanted users. The encryption and decryption keys are only known to users who are authorized to send and receive data through the encrypted channel. If both keys are identical, then the encryption method is called symmetric such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple-DES [2]. On the contrary, the Asymmetric method uses two different keys for encryption and decryption. Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman algorithm (RSA), and Elliptic Curve Cryptography (ECC) are good examples of such methods [3].

Many researchers have contributed to the area of enhancing the AES encryption algorithm. There are several criteria in this cryptographic algorithm that can be for optimizing or increasing the strength of the encryption and decryption process [20]-[21].

M.Vaidehi and B.Justus Rabi [4] examined and analyzed the AES-CBC mode for finding faults during the encryption process. They also compared this encryption mode with the AES-ECB mode showing that the initialization vector makes each ciphered message unique. However, the authors did not mention the source of the initialization vector before the encryption process.

C. Dewangan et al. [5] studied the avalanche effect in the Advanced Encryption Standard (AES) using binary codes. In this study, the encryption key and input plaintext are mapped into different binary codes before encrypting by the AES algorithm. The presented work resulted in a significant increase in the avalanche effect of the resulted ciphered word.

Daniel F. Garcia [6] evaluated the performance of the advanced encryption system. A systematic method is used to study the effect of configuration parameters on computational powers of the AES algorithm. Quantitative information has been obtained on the influence of the AES parameters on the performance of execution.

Flevina J. D'souza and D. Panchel [7] used a hybrid approach for Dynamic S-box Generation and Dynamic Key Generation. The study introduced mo complexity to the encryption process. Their implementation showed more diffusion and confusion in the resulted ciphertext.

Musliyana et al. [8] presented an approach of generating the encryption key based on time. The encryption key is generated randomly as a function of time while the sender logs the generation time to the system. The obtained results presented a higher security cipher key from the standard AES encryption method.

Sahmoud et al. [9] proposed a technique of producing different subkeys depending on the original encryption key.

The resulted sub keys are used in each round independently presenting more complexity to the encryption process.

Zhang et al. [10] used AES-CBC for fast encryption o image files. The proposed method divides the image into 128-bit blocks and then the first block is used as an initial vector for the encryption process. However, it is required to transmit the initial from the sender to the receiver to decrypt the encrypted image. Nevertheless, the method resulted in a high speed and secure encryption process.

Yu and Kim [11] depended on an unpredictable bio signal as a source of pseudorandom number generator. This method prevents the illegal users from predicting the next encrypted cipher key. The presented method depends on the unpredictable movement of the human body to generate the continuous sequence of random numbers ensuring that these numbers cannot be predicted with any computational algorithm.

II. AES Algorithm Basics

The principle of the AES algorithm depends on dividing the data stream into blocks of 128 bits and then encrypting each block with 128, 192, or 256-bit key. The method also named as Rijndael algorithm because of the developers J. Daemen and V. Rijmen [12]. The resulted blocks are arranged as matrices of 4x4 naming them states. The encryption process flow chart is shown in Fig. 1 and consists of the following processes [13]:

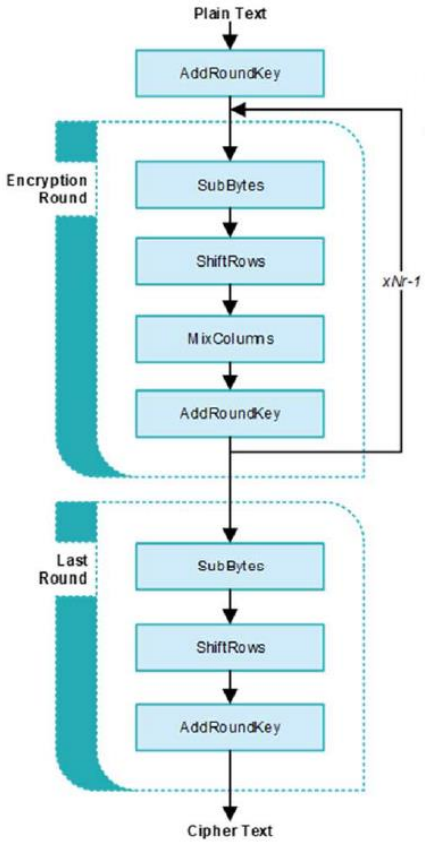

Fig. 1. Flow chart of AES encryption [13]

A. Substitute bytes:

A substitution table (s-box) is used to replace each byte. This operation has a high nonlinearity effect on the encryption process.

B. Shift rows:

The last three rows of the 4x4 byte matrix are shifted cyclically leaving the first row unaltered. This process adds more confusion and scrambling to the encryption process.

C. Mix columns

Considering every byte as a polynomial rather than a number, every column is multiplied by a fixed matrix satisfying the Galois Field (8th power of 2).

D. Add round key:

In this step, the XOR operation is implemented between the original input block and the round key.

The above explained encryption procedure represents the basic steps of AES. The process starts with add round key in which the key is XORed with the message matrix data block. Then, the four mentioned operations are applied to the data block completing a single round. The number of implemented rounds depends on the length of the encryption key. The number of rounds are 10, 12, or 14, for key lengths 128, 192, or 256 [14]. Finally, the ciphertext is produced after adding the round key again following the final round [4]. The decryption process is exactly the reverse of the encryption process.

Advanced Encryption Standard has six modes of operation. All AES modes have the same above mentioned steps but differ in further techniques. Cipher Block Chaining mode differs from other AES mode in depending on an Initialization Vector (IV) at the beginning of the encryption process. In this mode, the original message is added to the initialization vector before the encryption process [15]. Each block is encrypted depending on the IV of the previous block as shown in Fig. 2.

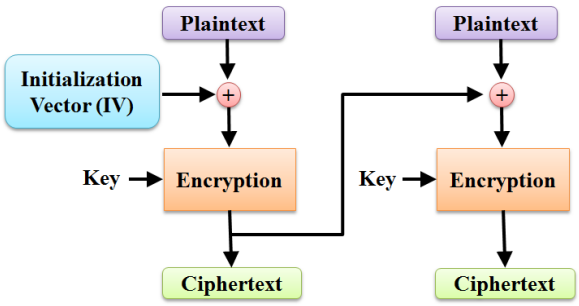

Fig. 2. Cipher Block Chaining mode encryption.

III. The Avalanche Effect

A desirable property that is used to evaluate cryptographic functions and block cipher algorithms is the avalanche effect. It measures the change in bits of the output as a function of change of bits in the input. In other words, it

evaluates how many bits are flipped in the output if one bit is flipped in the input. In high-quality encryption algorithms, a small change in the input plaintext or the encryption key results in a drastic alteration in the ciphertext. If the cryptographic algorithm fails to satisfy the avalanche effect to a certain degree, then it exhibits insignificant randomization and the input can be predicted depending only on the output. Furthermore, the repetitive process results in breaking the encryption algorithm completely. Therefore, it is desired to fulfill the avalanche effect consideration for algorithm designers.

In 1985, Webster and Tavares introduced the Strict Avalanche Criterion (SAC), which is a satisfactory condition of the avalanche effect where the output bits are 50% flipped with the change of a single input bit. This criterion examines the qualification of the encryption algorithm to withstand against undesirable attacks [16].

IV. Proposed Approach

In the proposed algorithm, the AES encryption method is modified in Cipher Block Chaining mode to increase the strength of encryption. The main problem arises from the fact that encrypting the same text repeatedly yields the same ciphertext. This is a major weakness in the encryption algorithm that exposes the hidden information into risk of decryption. A nonce number is required to generate different outputs at each encryption run. The real Unix time or Epoch time is used as an input to the initialization vector for each encryption process. The epoch time has a non-repeatable certain unique value at every moment ensuring that no repetition occurs in the future. In encryption algorithms, the encryption key is not exposed to unauthorized users for keeping the transferred information secret. Conversely, the initialization vector can be visible with no risks of affecting the privacy of the transferred data in a communication channel. Moreover, the Unix time exists in every digital system and is also transmitted through the global GPS [17]. Changing the IV continuously results in different encrypted messages each time without changing the encryption key. Additionally, the presented method is suitable for database systems with synchronized time or time-stamped systems.

The current Unix time consists of ten-digit numbers, which are used as the Initialization Vector that is having a 16 digit Hexadecimal number. The distribution of the time digits on the IV increases the strength of the encryption further. Only the sender and receiver are equipped with the correct arrangement of digits. This makes the ciphertext stronger than conventional AES-CBC mode. Fig. 3 shows the process of mapping Unix time to initialization vector before the encryption process. In this experiment, the three least significant digits are not used and constantly retain zero value.

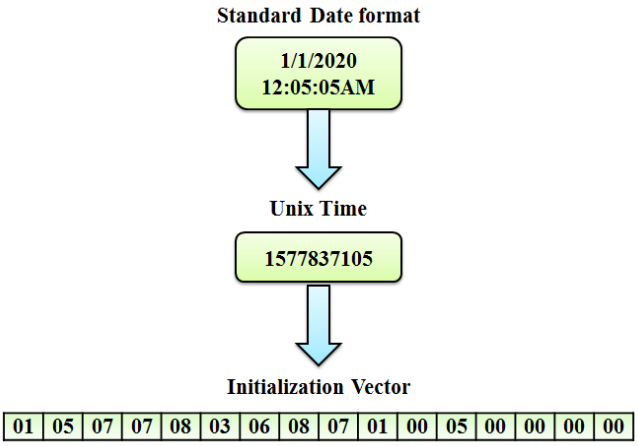

Fig. 3. Mapping Unix time to intialization vector.

These digits are spare and can be used for addressing or specific futuristic applications. On the other hand, the least significant digits in Unix time represent the continuous-time in microseconds which is changing instantly in real-time.

Each digit in Unix time has a certain period before ascending to the next value. This property can be implemented to validate the decryption process by embedding expiration date into the ciphertext. In other words, after a specific encryption time, the ciphertext is not decryptable and the decryption process results in an unreadable message.

V. Results and Evaluation

To evaluate the effect of the continuously changing IV on the AES encryption, several experiments are conducted repeatedly. Table I summarizes the first ten runs of the experiment and the avalanche effect of each resulted ciphertext with the corresponding Unix time. The detailed in sequence execution with time shows the variation of bits in the resulted ciphertext continuously with fluctuations on the avalanche effect above and below 0.5, as shown in Fig. 4. The results also showed that each ciphertext is generated as a new encryption process independent of the previous operation. Noting that the same input text message is used in all encryption procedures resulting in different outputs with Unix time.

TABLE I. AES-CBC Encryption with Unix Time

Message Type	Code	Avalanche Effect	Unix Time
Encoded Message	3132333435363738 3930616263646566	----	----
Encrytion Key	2B7E151628AED2A6 ABF7158809CF4F3C	----	----
Encrypt1	F82DC36294C2C4B5 B8060BFF0A59571C	0.52	1589031391862
Encrypt2	9EB8DE60604898D4 76E95D1BD91FD796	0.60	1589031391865
Encrypt3	2C6BAFEC1E51BA23 68CF252B6080649D	0.49	1589031391867
Encrypt4	B8332B4C26BA27F9 9F65836D32E658A4	0.38	1589031391869

Encrypt5	728390DB77AD44CC 1A74937880D68CAF	0.51	1589031391871
Encrypt6	1A1BA79AE2753817 8277E2182E2473DE	0.49	1589031391874
Encrypt7	1DF65645371309A5 AE229563A2474AC5	0.43	1589031391875
Encrypt8	CBD081E345666393 ECC19E78E339A6B6	0.52	1589031391877
Encrypt9	8A416C1D4029E397 0655DA06502B592B	0.59	1589031391878
Encrypt10	84B3DC858AF863B1 4D34AC708C7A94C4	0.52	1589031391879

To investigate the results further, a long time continuous experiment is executed for analyzing the statistics of the avalanche effect with time. Table II shows the results of calculations for a certain encryption runs. The outcomes show that the avalanche effect is between 0.33 and 0.66 with an average of 0.5. i.e., the number of bits that are changing with time for constant text input maintains a significant number.

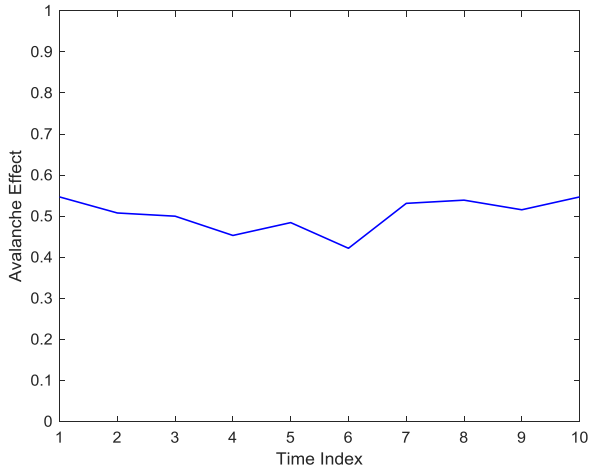

Fig. 4. Avalanche Effect with varying Unix time.

The calculations also show that this encryption method maintains the strict avalanche criteria for 53% of the time protecting the strength of the ciphertext [16]. Fig. 5 shows the dynamic change of the avalanche effect with time. Comparing the results with [8], the current approach has two advantages. First, the encryption key is kept unaltered, ensuring that the encryption and decryption process continuous perfectly. Second, there is no requirement for time login in two-way communication systems as the time digits are fed directly to the Initialization vector.

TABLE II. AVALANCHE EFFECT STATISTICS

Encryption runs	10000
Minimum	0.3359
Maximum	0.6641
Mean	0.5002
Standard Deviation	0.0439
Satisfies SAC	53.75%
Dissatisfies SAC	46.25%

Unlike [18] and [19], the suggested method does not require to add additional steps into the AES ciphertext generation. This gives the advantage of less memory usage in systems, higher security, and minimum modification at the same time.

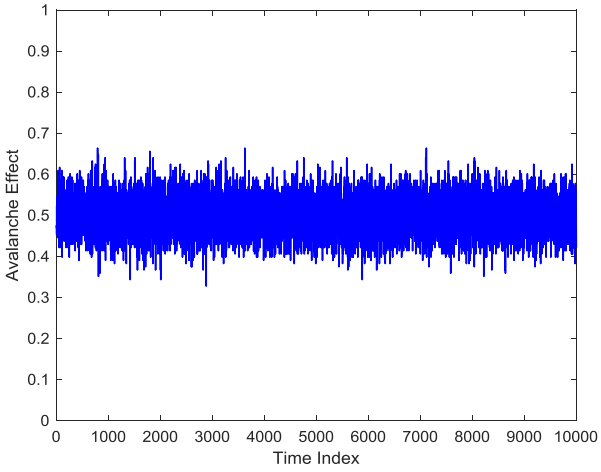

Fig. 5. Avalanche effect vs. time

VI. CONCLUSION

A new modified AES-CBC encryption algorithm that demonstrates higher security is presented in this paper. The structure of the proposed algorithm is updated from the original method by introducing Unix time parameter. The modified AES-CBC was evaluated using the Avalanche Effect criteria. The results show that the modified AES-CBC is higher security than the original and the previously modified AES-CBC algorithms. The ciphertext changes continuously with Unix time for the same input text while keeping the encryption key constant. Furthermore, the performance of modified AES-CBC satisfied the Strict Avalanche Criteria (SAC) more than 50 percent of the encryption time resulting in variable Avalanche Effect giving the algorithm higher encryption strength.

REFERENCES

[1] T. Park, H. Seo, J. Kim, H. Park, H. Kim, and C. H. Kim, "Efficient Parallel Implementation of Matrix Multiplication for Lattice-Based Cryptography on Modern ARM Processor," *Secur. Commun. Networks*, vol. 2018, 2018, doi: 10.1155/2018/7012056.

[2] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Comput. Sci.*, vol. 78, no. December 2015, pp. 617–624, 2016, doi: 10.1016/j.procs.2016.02.108.

[3] A. Kumar and N. Tiwari, "Effective implementation and evaluation of AES in Matlab," *Adv. Intell. Syst. Comput.*, vol. 176 AISC, no. VOL. 1, pp. 95–101, 2012, doi: 10.1007/978-3-642-31513-8_11.

[4] M. Vaidehi and B. J. Rabi, "Design and analysis of AES-CBC mode for high security applications," *2nd Int. Conf. Curr. Trends Eng. Technol. ICCTET 2014*, pp. 499–502, 2014, doi: 10.1109/ICCTET.2014.6966347.

[5] D. O. Vadaviya and P. Tandel, "Study of Avalanche Effect in AES," *Ncraes'15*, no. June, pp. 183–187, 2015.

[6] D. F. Garcia, "Performance Evaluation of Advanced Encryption Standard Algorithm," *Proc. - 2015 2nd Int. Conf. Math. Comput. Sci. Ind. MCSI 2015*, pp. 247–252, 2016, doi: 10.1109/MCSI.2015.61.

[7] 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*, vol. 2017-Janua, pp. 647–652, 2017, doi: 10.1109/CCAA.2017.8229881.

[8] Z. Musliyana, T. Y. Arif, and R. Munadi, "Security Enhancement Of Advanced Encryption Standard (Aes) Using Time-Based Dynamic Key Generation," *ARPN J. Eng. Appl. Sci.*, vol. 10, pp. 8347–8350.

[9] and A. S. Sahmoud S., Elmasry W, "Enhancement the Security of AES Against Modern Attacks by Using Variable Key Block Cipher," *Int. Arab J. e-Technology*, vol. 3, no. 1, pp. 17–26, 2013.

[10] Y. Zhang, Xueqian Li, and Wengang Hou, "A fast image encryption scheme based on AES," in *2017 2nd International Conference on Image, Vision and Computing (ICIVC)*, 2017, vol. 256, no. 104 Xi, pp. 624–628, doi: 10.1109/ICIVC.2017.7984631.

[11] H. Yu and Y. Kim, "New RSA encryption mechanism using one-time encryption keys and unpredictable bio-signal for wireless communication devices," *Electron.*, vol. 9, no. 2, pp. 1–10, 2020, doi: 10.3390/electronics9020246.

[12] J. Daemen and V. Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard," 2002.

[13] M. M. Mohd Nadzri, A. Ahmad, and A. Amira, "Implementation of Advanced Encryption Standard (AES) for Wireless Image Transmission using LabVIEW," *2018 IEEE 16th Student Conf. Res. Dev. SCOReD 2018*, pp. 1–4, 2018, doi: 10.1109/SCORED.2018.8710984.

[14] H. Lee, K. Lee, and Y. Shin, "Implementation and performance analysis of AES-128 CBC algorithm in WSNs," *Int. Conf. Adv. Commun. Technol. ICACT*, vol. 1, pp. 243–248, 2010.

[15] A. A. Abdelrahman, M. M. Fouad, H. Dahshan, and A. M. Mousa, "High performance CUDA AES implementation: A quantitative performance analysis approach," *Proc. Comput. Conf. 2017*, vol. 2018-Janua, no. July, pp. 1077–1085, 2018, doi: 10.1109/SAI.2017.8252225.

[16] A. F. Webster and S. E. Tavares, "On the Design of S-Boxes," in *Advances in Cryptology --- CRYPTO '85 Proceedings*, 1986, pp. 523–534.

[17] H. Y. Song and S. Hong, "Investigating Cyclic Visit Pattern of Mobility Through Analysis of Geopositioning Data," vol. 4, Springer International Publishing, 2019, pp. 589–602.

[18] Z. Rahaman, A. Diana, M. Akter, and A. Newaz, "A Novel Structure of Advance Encryption Standard with 3-Dimensional Dynamic S-box and Key Generation Matrix," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 2, 2017, doi: 10.14569/ijacsa.2017.080241.

[19] J. Alejandra, S. Chavarin, E. Christian, and B. Alvarez, "New S-box calculation approach for Rijndael-AES based on an artificial neural network," no. 2, 2017.

[20] S. B. Sadkhan, A. Salah, "The trade-off between security and quality using permutation and substitution techniques in speech scrambling system", 2019 First International Conference of Computer and Applied Sciences (CAS), pp:244-249.

[21] S. B. Sadkhan, D. M. Reda, "A Proposed Security Evaluator for Cryptosystem based on Information Theory and Triangular Game",2018 International Conference on Advanced Science and Engineering (ICOASE), pp: 306-311.