Enhanced AES algorithm based on 14 rounds in securing data and minimizing processing time

Noor Afiza Mohd Ariffin¹, Aymen Yousef Ahmed Ashawesh²

¹,²Department of Computer Science, Faculty of Computer Science & Information Technology, University Putra Malaysia, 43400 Serdang, Selangor, Malaysia

Abstract. Computer, Internet technology have grown exponentially, and constant evolution until today. The usage of digital data such as text, images, audio, animation and videos are commonly used in many aspects of daily activity. The continuous increase in the use of digital data transmission over a network and it exposed to the various kinds of attacks, unauthorized access and network hacking. Thus, it is very hard to ensure that the digital data transmission are secure from any attacks and unauthorized access especially for sensitive and important digital data. This has been raised researcher’s concerns on security of the digital data. Digital data security has become one of the most important aspects in communication. Cryptography is one of the most important technology for protecting digital data. As there is need for secure communication, efficient and secure cryptographic processing is needed for desirable platform overall performance. Improvement of any communication platform with secure and complicated cryptographic algorithms incredibly relies on ideas of data safety that is essential within the current technological global. This paper propose a Secured Modified Advanced Encryption Standard Algorithm with decreasing the rounds of Advanced Encryption Standard (AES) to 14 rounds in order to minimize encryption and decryption process time and increasing digital data security as well. The results have been proved that the proposed technique provides higher efficiency in term of encryption and decryption process time compared to other researches while increase security which has been proved by using avalanche effect test.

1. Introduction

In 21st Century, computer has turn out to be the crucial channel for human beings to speak each other, by means of sending, receiving, writing, modifying, uploading and downloading via Internet and cause it to rise up the security problem in Internet communication. They may fear whether or not the documents and information can be sent in a secure manner or not? consequently, it needs to be the compulsory which all of the documents and data sent thru the web need to be secured and guarded due to the fact each person is worried about the sensitive data to the internet and most companies consider that internet isn't as safe as their own data centers [1]. Consider that how much it information or data is probably worth going? So others more expert person was already knew this form of hassle can be bringing in internet in order that they had investigative type of encryption algorithm to resolve this problem. Therefore, an encrypted communication can be carried out that is available between sender and receiver, without being visible or attacked by means of the unauthorized third party [2].

AES encryption is an algorithm used to encrypt in addition to decrypt information electronic transmission of information safety functions. Furthermore, AES algorithm permits the usage of cipher
key which are 128, 192, or 256 bits long and additionally that are to defend the 16-byte blocks in the information encryption key [3].

With AES encryption and decryption are carried out the usage of the identical key so this is referred to as a symmetric encryption algorithm. While encryption algorithm makes use of in different keys, which can be one public and one private which is known as asymmetric encryption algorithm. The data encryption keys used within the encryption process is a binary string. it is due to the fact the ones are using the same encryption key to encrypt and decrypt the information, it is vital to hold a secret encryption key, and use the keys tough to guess. A few key technology software used for this precise task. Every other approach is derived from a passphrase key. At the same time as a good encryption platform was never used separate passphrase as the encryption key [4].

Furthermore, the advanced Encryption standard (AES) algorithm is a symmetric block cipher that makes use of a symmetric key can be 128, 192, or 256 data blocks of 128 bits encryption. AES encrypted the information block while procedure encryption in 10, 12 and 14 rounds that it relies on the key length. AES encryption is fast and flexible [5].

2. Related Work

This section is including the work done by the several researchers in the field of Advance Encryption Standard (AES) cryptographic algorithm for data security. However, critical analysis has been carried out and finally the observations have been shown as well.

[7], the authors effectively optimized the AES algorithm via offering a novel approach that involved Shift Row and S-box changes to map the mixture Column transformation. This approached removed the Sub Bytes feature. The outcome of their experiments confirmed that each encryption and decryption techniques an enhancement of 87% and 14% respectively.

[8] Proposed a substitution box that uses the RC4 key schedule algorithm (KSA). The ensuing matrix is a Key dependent S-box based totally that is dynamically generated based from a few key built the usage of RC4. The RC4-generated S-box was used to replace the Rijndael S-box at some point of the encryption and decryption processes.

[9] Proposed some other Key structured S-box aimed at substituting the Rijndael S-box. In their paper, they modified the AES cipher by using putting every other segment in the beginning of the round feature. They name the extra segment as the S-box Rotation that rearranges via rotating the original S-box consistent with a round key. The round key was derived the use of the key schedule algorithm. The rotation value is dependent on the whole round key. Their experiments confirmed that the enhancement on the unique AES did not violate the security characteristics whilst in addition introduced confusion without violating the diffusion characteristic.

[10] Worked on overall performance analysis of cryptographic algorithms: DES and AES. Those algorithms takes big quantity of computing resources including simulation time memory utilization and degree of encryption are of main challenge. In AES, impact is excessive in comparison with the DES which is used in the financial software. The more research has achieved within the field of picture and offer more protection to the system.

[11] Worked on making use of low power method in AES mix Column Inverse mix Column transformation. They inspect using low power resources which increases the security wishes and performance. As a result, the information paths which are of no use for the platform are deactivated and increase the ability of the platform for the higher outcomes.
[12] Worked on excessive definition image encryption algorithm primarily based on AES modification. They evaluated block cipher algorithm widely recognized AES as it is more secure. The major challenge of this scheme was the encryption/decryption time required was more and the assaults on the encryption algorithm can decreased the rounds.

[13] Proposed a Key-based S-box (AES-KDS) to make the AES algorithm stronger. The encryption and decryption procedure AES-KDS is just like the unique AES cipher as to the number of rounds, information and key size. Each round features in the modified model resembles that of original AES, however is composed of five levels instead than 4 levels. The more level named Rotate S-box is delivered at the beginning of every round feature. The other 4 levels continue to be the same. But, for the decryption procedure there are only 4 levels similar inside the authentic cipher. But the Inverse Sub-Bytes operation is modified to opposite the impact of the Rotate S-box operation formerly carried out in the encryption procedure. That's accompanied via an outline of key expansion and era of shift offset-matrix.

3. Secured Modified Advanced Encryption Standard Algorithm

In order to conquer the issue of excessive calculation and computational overhead, we examined the advanced Encryption standard (AES) and modify it, to minimize the calculation of algorithm and for enhancing the encryption performance. So we developed and enforce a modified AES based totally algorithm for all type of records. The primary goal to modify AES is to offer much less computation and better security for information. The modify AES algorithm adjusts to offer higher encryption speed. In modified-AES the block duration and the key duration are specified consistent with AES. We anticipate a key length of 256 bits that is generally carried out. In modified-AES encryption and decryption procedure resembles to that of AES, in account of variety of rounds, records and key size. The round feature includes 4 levels. To conquer the issue of high calculation we pass the Mix-column step and add the permutation step. Mix-column offers higher safety however it takes big calculation that makes the encryption algorithm slow. The opposite 3 levels continue to be unbothered as it is inside the AES.

There are 4 operational blocks which constitute one round of modified-AES. There are 14 rounds for complete encryption. The following are 4 levels that we use for modified-AES algorithm which are:

- Substitution bytes
- ShiftRows
- Permutation
- AddRoundKey

Substitution Bytes, ShiftRows and AddRoundKey continue to be unaffected as it is inside the AES. Right here the crucial feature is Permutation that is used rather than Mix-column. Permutation is broadly utilized in cryptographic algorithms. Permutation operations are thrilling and crucial from each cryptographic and architectural points of view. Modified-AES algorithm takes 256 bits as input. The features Substitution Bytes and ShiftRows also are interpreted as 256 bits while the Permutation feature also takes 256 bits. Inside the permutation table every access shows a particular role of a numbered input bit can also include 256 bits in the output.

For the overall decryption of modified-AES algorithm the transformation procedures are, Inv-Bytesub, Inv-Shiftrows, Inv-Permutation, and the Addroundkey, that are carried out in 14 rounds as it is in the encryption procedure [6]. So, modified-AES algorithm with 14 rounds will be used to encrypt and decrypt any data file in proposed system (Secured Modified AES System). Bit Permutation used for encryption process while inverse bit permutation used for decryption process of data files. The following is structure of modified AES algorithm in figure 1 above:
4. Algorithm Evaluation Based on Encryption Throughput

Throughput of any encryption algorithm is the size of document (file) encrypted over unit time for encryption. So, if the value of encryption throughput is high then it means the algorithm is fast and suitable for encryption. However, encryption throughput of any decryption algorithm is the size of document (file) which about to be decrypted over unit time of decryption. So, if the value of throughput is high then it means the algorithm is fast and suitable for decryption.

\[ \text{Encryption Throughput} = \text{file size} / \text{time} \]

Once the user uploaded the data into proposed system then the user can click a button for analysis. Execution time of different several file size for different encryption techniques have been recorded. There are 5 encryption techniques used for this analysis which are DES, 3DES, AES, twofish and proposed Modified algorithm as shown below. Therefore, it proved that the proposed Modified algorithm consumes less time for all the file.
Table 1: Encryption execution time for different file

| Input file size (kb) | Encryption execution time (s) |
|----------------------|------------------------------|
|                      | DES  | AES  | 3DES | Proposed Modified | Twofish |
| 2                    | 21   | 24   | 22   | 15               | 25       |
| 3                    | 64   | 72   | 61   | 40               | 75       |
| 4                    | 135  | 143  | 130  | 125              | 139      |
| 5                    | 278  | 291  | 254  | 240              | 225      |
| 6                    | 460  | 481  | 441  | 425              | 470      |
| 7                    | 655  | 692  | 613  | 598              | 699      |

Figure 2. Execution time graph
Table 2: Decryption execution time for different file size.

| Input file size (kb) | Decryption execution time (s) | DES | AES | 3DES | Proposed Modified | Twofish |
|----------------------|-----------------------------|-----|-----|------|-------------------|--------|
| 2                    |                             | 21  | 24  | 22   | 15                | 25     |
| 3                    |                             | 64  | 72  | 61   | 40                | 75     |
| 4                    |                             | 135 | 143 | 130  | 125               | 139    |
| 5                    |                             | 278 | 291 | 254  | 240               | 225    |
| 6                    |                             | 467 | 471 | 437  | 425               | 470    |
| 7                    |                             | 655 | 692 | 613  | 598               | 699    |

Figure 3: Decryption process time

5. Analysis of Proposed Technique Based on Throughput Execution Time and Performance
In this section, analysing how much good proposed system mentioned about security issues which comes from the storage and encryption techniques of user's personal data. However, this thesis elaborated privacy concerns which can happened when storing data into database without great encryption techniques. Privacy of user data is crucial, so that, the proposed system has option to encrypt data (personal or office data) by using Modified advanced encryption standard algorithm by using 14 rounds before upload to the database.

Avalanche Effect
This test involves with proposed technique (Modified Advanced Encryption Standard Algorithm) and testing file or text message. The author of this thesis used proposed technique (Modified Advanced Encryption Standard Algorithm) for minimize encryption and decryption processing time while increases level of security of users data and data files. The author of this journal paper used avalanche effect test to check if the proposed system is much secured. The following are results obtained from testing proposed system.
### Table 3: Results after testing avalanche effect

| ROUND | Number of flipped bits | Avalanche Effect (%) |
|-------|------------------------|----------------------|
| 1     | 59                     | 46.09%               |
| 2     | 65                     | 51%                  |
| 3     | 68                     | 53.2%                |
| 4     | 67                     | 52.3%                |
| 5     | 68                     | 53.2%                |
| 6     | 64                     | 50.09%               |
| 7     | 67                     | 52.3%                |
| 8     | 72                     | 56.25%               |
| 9     | 69                     | 53.91%               |
| 10    | 71                     | 55.5%                |
| 11    | 74                     | 57.81%               |
| 12    | 69                     | 53.91%               |
| 13    | 75                     | 58.59%               |
| 14    | 73                     | 57.03%               |
Based on results obtained in avalanche effect test, the average amount of avalanche effect of all rounds using in proposed technique is more than 50% which proved that the proposed system (Secured Modified AES System) secured. So, the user’s data of proposed system will be secured.

6. Conclusion
Digital data security has become one of the most important aspects in communication. Cryptography is one of the most important technology for protecting digital data. As there is need for secure communication, efficient cryptographic processing is needed for desirable platform overall performance. Improvement of any communication platform with secure and complicated cryptographic algorithms incredibly relies on ideas of data safety that is essential within the current technological global. Based on that, this research proposed secured Modified Advanced Encryption Standard by decreasing the number of rounds (Nr) to 14 rounds for encryption and decryption data file make more secure and efficient.

References

[1] F. R. C. N.-H. 15. C. S. 2019 Spellman, Information technology protection and homeland security, 2019.
[2] “2019 International Conference on Computing, Networking and Communications, ICNC 2019,” 2019 International Conference on Computing, Networking and Communications, ICNC 2019, 2019.
[3] K. P. Singh and S. Dod, “An Efficient Hardware design and Implementation of Advanced Encryption Standard ( AES ) Algorithm,” Spec. Issue Int. J. Recent Adv. Eng. Technol. Technol. Manag. ISSN (Online, 2016.
[4] D. F. Garcia, “Performance Evaluation of Advanced Encryption Standard Algorithm,” in Proceedings - 2015 2nd International Conference on Mathematics and Computers in Sciences and in Industry, MCSI 2015, 2016, doi: 10.1109/MCSI.2015.61.
[5] M. A. Ako, “Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data,” Cryptogr. Netw. Secur., 2017.
[6] H. V. Gamido, A. M. Sison, and R. P. Medina, “Modified AES for text and image encryption,”
Indones. J. Electr. Eng. Comput. Sci., 2018, doi: 10.11591/ijeecs.v11.i3.pp942-948.

[7] R. Riyaldhi, Rojali, and A. Kurniawan, “Improvement of Advanced Encryption Standard Algorithm with Shift Row and S-Box Modification Mapping in Mix Column,” in Procedia Computer Science, 2017, doi: 10.1016/j.procs.2017.10.079.

[8] K. Kazlauskas, G. Vaičekauskas, and R. Smaliukas, “An Algorithm for Key-Dependent S-Box Generation in Block Cipher System,” Inform., 2015, doi: 10.15388/Informatica.2015.38.

[9] A. Alabaichi and A. I. Salih, “Enhance security of advance encryption standard algorithm based on key-dependent S-box,” in 2015 5th International Conference on Digital Information Processing and Communications, ICDIPC 2015, 2015, doi: 10.1109/ICDIPC.2015.7323004.

[10] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, “A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish,” in Procedia Computer Science, 2016, doi: 10.1016/j.procs.2016.02.108.

[11] B. Bilgin, B. Gierlichs, S. Nikova, V. Nikov, and V. Rijmen, “A more efficient AES threshold implementation,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2014, doi: 10.1007/978-3-319-06734-6_17.

[12] S. M. Wadi and N. Zainal, “High Definition Image Encryption Algorithm Based on AES Modification,” Wirel. Pers. Commun., 2014, doi: 10.1007/s11277-014-1888-7.

[13] S. Arrag, A. Hamdoun, A. Tragha, and E. Khamlich Salah, “Implementation of stronger AES by using dynamic S-box dependent of master key,” J. Theor. Appl. Inf. Technol., 2013.

[14] A. R. Pratama, “Belajar UML - Use Case Diagram,” Codepolitan, 2019.

[15] F. H. Nejad, S. Sabah, and A. J. Jam, “Analysis of avalanche effect on advance encryption standard by using dynamic S-Box depends on rounds keys,” in 2014 International Conference on Computational Science and Technology, ICCST 2014, 2014, doi: 10.1109/ICCST.2014.7045184.

Acknowledgments
Special thanks from authors for financial support from Universiti Putra Malaysia.