ISSN 2347 - 3983

Volume 8. No. 10, October 2020

International Journal of Emerging Trends in Engineering Research

Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter808102020.pdf

https://doi.org/10.30534/ijeter/2020/808102020

# AN ENHANCED CRYPTO ALGORITHM FORSECURE DATA STORAGE USING AES ALGORITHM

**Caroline Kalaiselvi. R[1] , Dr. Mary Vennila.S[2],**

[1] Research Scholar, PG and Research Department of computer science,
Presidency College, Chennai, India, carrie.jonna@gmail.com

[2]Associate Professor, Head & Research Supervisor,
PG & Research Department of Computer Science, Presidency College, Chennai,India,
vennilarhymend@yahoo.co.in

## ABSTRACT

Are data-security & data-integrity during existence of a challenger. Based on data-security needs and data-threats implicated different crypto-graphic technologies which similar to symmetric-key or public-key cryptography which used while transportation and data-storage.

It is common knowledge that countless professionals continue to access the cloud for various requirements and from the point of view of absolute security of the cloud computing that needs to be insulated from exogenous threats to the data involved, a process of encoding using the Enhanced Advanced Encryption Standard (CAES) to protect the data before its release in the cloud becomes a golden standard of protocol now to safeguard the data.

**Key words:** Cryptographic methods, AES, RSA, Blowfish.

## 1. INTRODUCTION

### 1.1 AES-Algorithm:

NIST mentioned latest advanced-encryption-standard might become block-cipher, proficiently managing 128-bit blocks with keys of 128, 192 and 256-bits chosen as a further advancement in the encryption standard algorithm included:

**Security:** Such algorithms should be fashioned impenetrable to cyber vandalism in whatever form it is designed for its nefarious outcome.

**Cost:** Planned for a global outreach, it is not exclusive and does not entail royalty, the algorithms have been evaluated for efficacy in both the fronts of computation as well as the memory.

**Implementation:** The operational characteristics of the algorithm such as flexibility, its functionality in the hardware and software spheres and its overall simplicity in implementation have been evaluated.

Advanced-Encryption-Standard comprises 3 block-ciphers AES 128, 192 and 256 bits and cryptographic keys of these bits are used for both encryption and decryption. The “Rijdael cipher” recognizes extra block sizes and key lengths, but for Advanced-Encryption-Standard, individual methods will not suffice.

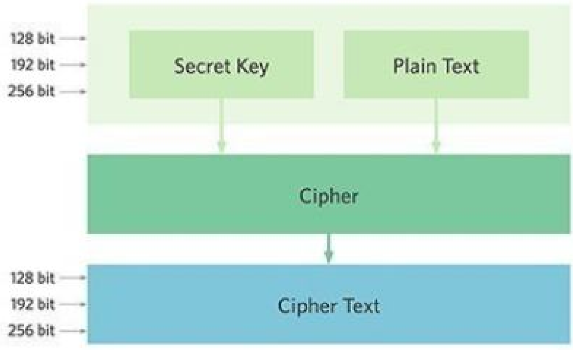

**Figure. 1.** AES-Algorithm Design

Figure 1 explains the Algorithm design of AES. Symmetric-ciphers use same key meant for both encryption and decryption may tend to familiarize both the data sender and the receiver in the utilization of the secret key[1]. Entire key lengths enough in protecting classified data upon "Secret" level along with "Top-Secret" data requiring 192-bit or 256-bit key lengths. In Advanced-Encryption-Standard, total rounds were estimated by key lengths – 10 rounds for 128-bit keys, 12-rounds for 192-bit keys and 14-rounds for 256-bit keys.

Single-round consist numerous steps for processing which comprise replacement and combination of plaintext & renovate it with final output of cipher text.

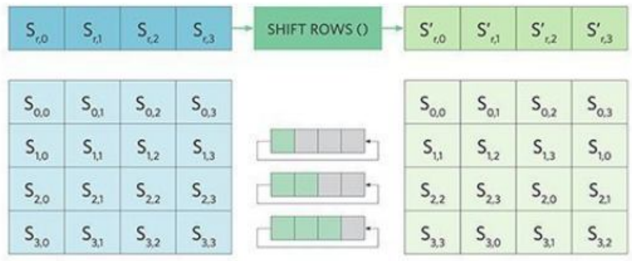
$S_{r,0}$ $S_{r,1}$ $S_{r,2}$ $S_{r,3}$
SHIFT ROWS ()
$S'_{r,0}$ $S'_{r,1}$ $S'_{r,2}$ $S'_{r,3}$
$S_{0,0}$ $S_{0,1}$ $S_{0,2}$ $S_{0,3}$
$S_{1,0}$ $S_{1,1}$ $S_{1,2}$ $S_{1,3}$
$S_{2,0}$ $S_{2,1}$ $S_{2,2}$ $S_{2,3}$
$S_{3,0}$ $S_{3,1}$ $S_{3,2}$ $S_{3,3}$
$S_{0,0}$ $S_{0,1}$ $S_{0,2}$ $S_{0,3}$
$S_{1,1}$ $S_{1,2}$ $S_{1,3}$ $S_{1,0}$
$S_{2,2}$ $S_{2,3}$ $S_{2,0}$ $S_{2,1}$
$S_{3,3}$ $S_{3,0}$ $S_{3,1}$ $S_{3,2}$

**Figure. 2.** AES Transformation Setup

Figure 2 gives the transformation setup of AES. First revolution within Advanced-Encryption-Standard cipher was exchange of data using a changeover table; 2nd revolution was shifting data rows, 3rd mixes columns. Final one is simple, special or or XOR performed in in every column utilizing dissimilar part of encryption key[2].

## 2. PERFORMANCE EVOLUTION OF DATA SECURITY

Major concern with Advanced-Encryption-Standard, a-symmetric algorithm; requires encryptor and decryptor which utilize same-key. Provides increase in crucial key management issues – how can all important secret-keys distributed to hundreds of recipients around world without running at massive risk. Answer is combine strengths of Advanced-Encryption-Standard and Rivest-Shamir-Adleman.

Most modern communication environments, including the Internet, are encrypted by a fast Advanced-Encryption-Standard algorithm to exchange bulk data. Registered recipients publish public key to access the secret key needed to decrypt the information while maintaining a related private key that only they know. Sender afterwards utilizes public-key & Rivest-Shamir-Adleman encrypts and transmits data to every recipient, their own secret- key of Advanced-Encryption-Standard used to decrypt data[3].

Major aim of research work is to prove Custom Advanced-Standard-Encryption(CAES) algorithm is much more efficient than previous AES-algorithm. Comparison of different cryptographic algorithms could produce an efficient solution for data security. Better understanding of crypto-graphic algorithms could improve Quality of Service (Qos), and provide as a barrier for data-security, data-theft, etc[4].

## 3. PURPOSE OF THE STUDY

The main objective of the work is,

(i) Implement cryptographic techniques to sensitive-data of application such as password field, photo, etc.

(ii) Applications should restrict data-theft which is being induced by attackers or man-in-the-middle.

(iii) Find out best crypto-graphic technique from being configured ones in application level. With help of parameters such as performance, efficiency, accuracy, etc encryption & decryption being performed.

(iv) To further enhance the efficiency by using Advanced-Standard-Encryption (AES) Approach.

## 4. DEVELOPMENT OF AES 256-BIT ALGORITHM

It is correct that 256-bit key on most count makes guessing difficult and that could be the reason why it is called brute-force-attack as opposed to the vulnerability of using the 128-bit key. To produce brute-force attack, hackers require quantum-computing and their most likely target could be a weakest link to access the data stored side-stepping the safeguards in place. Here, notwithstanding the 128-bit keys or the 256-bit keys encryptions, a vulnerable software that is not well primed to ward off any cyber-attack, when the location of the storage is compromised and when the system administration is not in the hands of a person of proven acumen, it becomes open sesame for a hacker to have a field day in cyber-attack.

Attacks against AES 256-bit key is impracticable what with 2100 steps of computation, it is well beyond the realm of feasibility no matter how many supercomputers one may deploy!!!. So, this precludes attack against the 256-bit key protection. Practically, those claims of cyber-attacks on the 256-bit key lack validation from a practical point of view and therefore does not make the system prone to such attacks.

## 5. DEVELOPMENT OF CUSTOM AES ALGORITHM (CAES)

Custom-AES(CAES) is also a-symmetric encryption-algorithm and it is being derived from ‘”AES-algorithm’”. Custom ‘”AES-algorithm’” encryption-algorithm allows 128-bit, 192-bit encryption and 256-bit encryption. Symmetric-encryptions extremely much faster when evaluated with asymmetric-encryption and are integrated in systems such as database system. Following online-tool generates ‘”AES” encrypted-password and decrypt ‘”AES” encrypted-password.Custom ‘”AES-algorithm’” provides two dissimilar mode of encryption and decryption Electronic Codebook& Cipher Block Chaining mode.

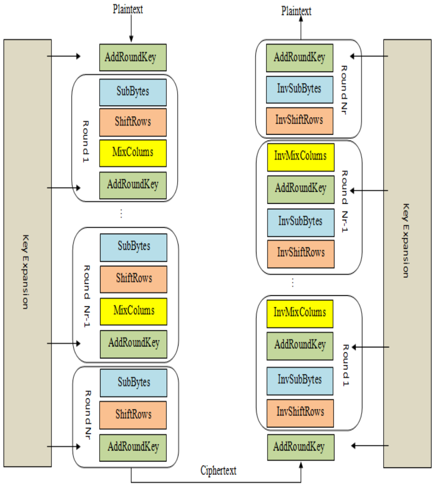

**Figure.3.** AES system-Architectural Diagram

Figure 3 demonstrates the AES system diagram. Difference between Custom-AES-algorithm 128-bit & 256-bit data-encryption is very technical one. According to experts prediction, “’Custom-AES-128’” bit will be secure and un-crackable for at least next ten years or so. It’s apparent “’Custom-AES-256’” bit much stronger than “’AES-128’” bit, so that only for our experimental evaluation we had implemented it. End-users require magnitude orders, extra bits key-length for your own peace mind, gets 256-bit data-encryption.

In Custom-AES-algorithm, five set of parameters such cipher mode, block size, secret key length, IV key length and salt generation length are taken into account to estimate performance of Custom-Advanced-Standard-Encryption algorithm and compared with existing works, like Advanced-Standard-Encryption algorithm[5]. Major aim of research work is to prove Advanced-Standard-Encryption (AES) algorithm is much more efficient than previous Rivest-Shamir-Adleman and Blowfish-algorithm. Comparison of Custom-AES-algorithm and AES-algorithm encryption-algorithms could produce an efficient solution for data-security. This approach has very soundrealistic knowledge of crypto-graphic technique and outcome of proposed-research will reduce time-consumption during encryption-process and improved security level during decryption-process too.

## 6. EXPERIMENTAL EVALUATION

For experimental discussions, five set of parameters such cipher mode, block size, secret key length, IV key length[6] and salt generation length are taken into account to estimate performance of Advanced-Standard-Encryption (A-E-S) algorithm and compared with existing work Custom AES Algorithm.

Analytical evaluation and experimental analysis are conducted for proposed-techniques and private-data which is used by end-user for encryption- process and decryption-process for files in software-application are tracked. Later stored analytics-data being analysed for crypto-graphic process accuracy and efficiency. Encryption efficiency is improved by 5-15% compared to existing or previous works.

Obtained results show AES-Algorithm compared with performance of other 2 different encryption-algorithms Blowfish-Algorithm and RSA-Algorithm has recorded high encryption and decryption success-rate. Recorded analytics statistics against every algorithm will be plotted into a graph and displayed in software-application. Future indispensable parameters of AES-Algorithm such as key-size, block-size, cipher-mode, etc. will be modified to make more accurate. These steps towards AES-Algorithm will increase crypto-graphic intensity, which will ultimately boost intensity of security in cloud-environment.

With help of these sorts of recorded data, the parameters of AES-Algorithm such as block-size, secret-key size, salt-size and cipher-mode have been fine tuned. These changes made in AES-Algorithm have resulted in increased security level, accuracy, efficiency, etc.

**Table 1:** Tabulation of Encryption Time

| No. of files | ENCRYPTION TIME | |
|---|---|---|
| | CUSTOM AES | AES |
| **2** | **0.1** | **0.1** |
| **4** | **0.19** | **0.2** |
| **6** | **0.29** | **0.27** |
| **8** | **0.28** | **0.28** |
| **10** | **0.49** | **0.49** |
| **12** | **0.68** | **0.58** |
| **14** | **1.04** | **1.14** |
| **16** | **1.1** | **1.18** |

Encryption time of Custom AES-Algorithm is compared with existing AES Algorithm as shown in table 1.

We should be very careful while changing encryption padding, because it will result in error while process file during encryption and decryption process. It will in fact affect accuracy level of AES-Algorithm and turn into a hurdle for the end-user data which is being stored into cloud-storage in any sort of cloud-environments[7]. By making changes in encryption padding and cipher mode then only we can able to change block size of AES-Algorithm from 16-bit to 32-Bit. Above process will enhance security level of AES-Algorithm and in-turn produces better results during encryption and decryption process. Obtained results are tabulated above to show case encryption time vs. number of files[8].

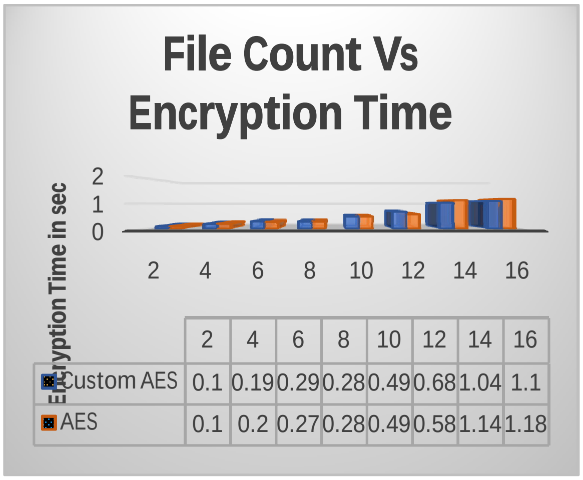

**Figure 4**. No. of Files vs. Encryption Time

Figure4. describes time taken for encryption of number of files by Custom AES-Algorithm is compared with existing AES Algorithm.

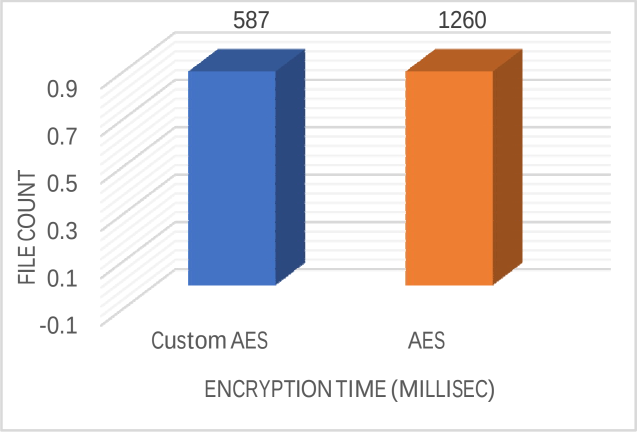

**Figure 5.** No. of Files vs. Encryption Time in Milliseconds

Figure 5 describes the time taken for encryption of number of files by Custom AES-Algorithm is compared with existing AES Algorithm using a chart. Captured data while processing encryption of files will be plotted into a graph against time taken for encryption and number of total files processed by end-users. Failures such as incorrect-key, padding-error, incorrect salt-size, incorrect block-size, etc. are also captured. But these sorts of data are not considered during plotting graph. Only we had plotted success cases into graph in order to display time taken for encryption alone, because if we plot failure cases the time taken for encryption will be zero and it looks like it had provided more efficiency.

## 7. MEASURE OF DECRYPTION EFFICIENCY

Experiment conducted with 'n' number of files uploaded by end-user's are being decrypted by major algorithm such as AES-Algorithm. End-user chooses desired decryption-algorithm which they are going to use during registration itself. Performance of all these algorithms during decryption -process of every file has been noted down. With help of these sorts of recorded data, the parameters of AES-Algorithm such as block-size, secret-key size, salt-size and cipher-mode have been fine tuned. These changes made in AES-Algorithm have resulted in increased security level, accuracy, efficiency, etc.

**Table 2 :** Tabulation of Decryption Time

| No. of files | DECRYPTION TIME | |
|---|---|---|
| | CUSTOM AES | AES |
| **2** | **0.1** | **0.1** |
| **4** | **0.2** | **0.22** |
| **6** | **0.22** | **0.26** |
| **8** | **0.21** | **0.27** |
| **10** | **0.41** | **0.43** |
| **12** | **0.62** | **0.64** |
| **14** | **1.14** | **1.17** |
| **16** | **1.12** | **1.19** |

Decryption time of Custom AES-Algorithm is compared with existing AES Algorithm as shown in table 2.

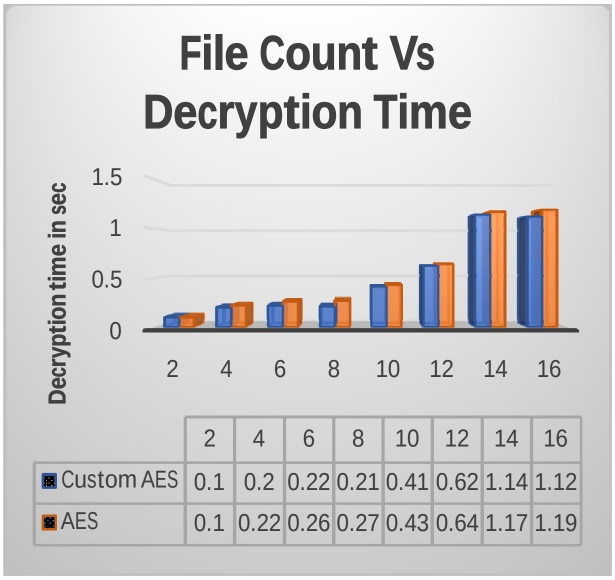

**Figure 6.** No. of Files vs. Decryption Time

Figure 6. describes time taken for decryption of number of files by Custom AES-Algorithm is compared with existing AES Algorithm.

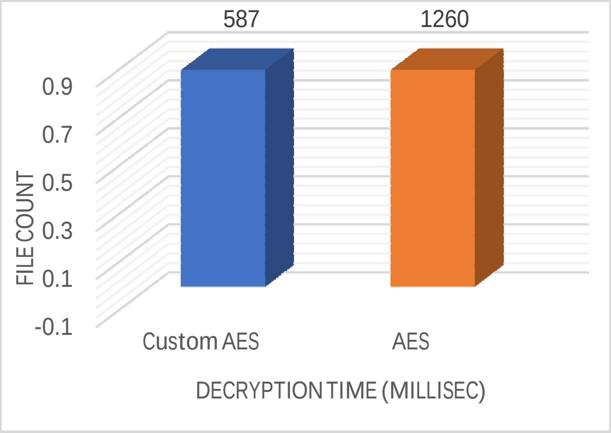

**Figure 7.** No. of Files vs. Decryption Time in Milliseconds

Figure7 describes time taken for decryption of number of files by Custom AES-Algorithm is compared with existing AES Algorithm.

Captured data while processing decryption of files will be plotted into a graph against time taken for decryption & number of total files processed by end-users. Failures such as incorrect-key, padding-error, incorrect salt-size, incorrect block-size, etc. are also captured. But these sorts of data are not considered during plotting graph. Only we had plotted success cases into graph in order to display time taken for decryption alone, because if we plot failure cases time taken for encryption will be zero and it looks like it had provided more efficiency.

## 8. CONCLUSION

We had developed a software application like Google-Drive which stores and retrieve files from cloud-severs. Prior registering into application users should select any one of crypto-graphic algorithm and set private-key & public-key too. After administrator verified all mandatory details of user, then only user can able to login to application & perform any other process such as uploading or downloading files. This approach has very sound practical knowledge of promoting cryptographic techniques. Outcome of this research paper will reduce headache of application team from data theft.

Major aim of this paper work prove Custom-Advanced-Standard-Encryption (CAES) algorithm much more efficient than AES. Evaluation of different cryptographic-algorithms could produce an efficient solution for data-security. Better understanding of crypto-graphic algorithms could improve Quality-of-Service (Qos), and provide as barrier for data-security, data-theft, etc.

## REFERENCES

1. Abha Sachdev, Mohit Bhansali, "Enhancing Cloud Computing Security using AES Algorithm", International Journal of Computer Applications, pp. 0975 – 8887, 2013.
2. Smitha Nisha Mendonca, "Data Security in Cloud using AES", Cloud Computing, International Journal of Engineering Research & Technology on (Volume: 07, Issue: 01) January-2018.
3. Prof.S.Delfin, Rachana Sai.B, Meghana J.V, Kundana Lakshmi.Y, Sushmita Sharma., "Cloud Data Security Using AES Algorithm" International Research Journal of Engineering and Technology on Cloud Computing, October 2018.
4. Hala Bahjat AbdulWahab, Abdul Monem S.Rahma., "New Quantum Cryptography System Using Quantum Description techniques for Generated Curves," International conference on security and management, July 2009.
5. Henk C.A. van Tilborg, Eindhoven, "Encyclopedia of Cryptography and Security", Springer Science + Business Media, January 2012.
6. B.Schneier, "Description of a New Variable Length Key" Cambridge Security Workshop Proceedings on Cloud Computing, December 1993.
7. Chen, Yao, and Radu Sion. "On securing untrusted clouds with cryptography. "Proceedings of the 9th annual ACM workshop on Privacy in the electronic society. ACM, 2010.
8. Agudo, Isaac and Nuez, David and Giammatteo, Gabriele and Rizomiliotis, Panagiotis and Lambrinoudakis, Costas. Cryptography Goes to the Cloud. In Lee, Changhoon and Seigneur, Jean-Marc and Park, James J. and Wagner, Roland R., editors, Secure and Trust Computing, Data Management, and Applications, pages 190–197, Springer Berlin Heidelberg, 2011.