ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Efficient Data Encryption by Combining AES Encryption Approach with Pattern Conversion and Parallel Execution Concepts

Nagma, Bhupesh Dewangan

M.Tech Student, Department of Computer Science & Engineering, CSIT, Bhilai (C.G.), India

Assistant Professor, Department of Computer Science & Engineering, CSIT, Bhilai (C.G.), India

ABSTRACT: Protecting sensitive information is that the ultimate goal of virtually all IT security measures. Two robust arguments for shielding sensitive information aim to avoid fraud and to guard privacy. Cryptography is a methodology of storing and transmission information in an exceedingly specific form those who are supposed access it. This method involves converting plain text into cipher text in an exceedingly method referred to as coding, then back once more to plain text employing a method called decoding. Encryption/decryption can be quite effective while sensitive dealing, like a credit-card purchase on-line, or the discussion of an organisation secret between totally different departments within the organisation. The stronger the cipher is, the more durable it's for unauthorised individuals to interrupt it. However, because the strength of encryption/decryption will increase, therefore will the price. many alternative encoding strategies are planned to stay the protection of the information. This paper proposes an improved AES (Advanced Encryption Algorithm) by utilising the ideas of parallel execution techniques and then the quality of encrypted information is improved by employing symbolic pattern generation techniques. The approach is cost effective, quick and safer for data transmission.

KEYWORDS: Encryption, Decryption, AES, Parallel Execution Technique, Pattern Representation

I. INTRODUCTION

Cryptography is that the science of creating communication unintelligible to everybody except the meant receiver(s). It's the study of ways of converting messages in a form so solely meant recipients will be able to decode it and browse the message. Cryptography offers economical answer to safeguard sensitive data during a sizeable amount of applications together with personal information security, web security, diplomatic and military communications security, etc. through the processes of encryption/decryption. A cryptosystem could be a set of algorithmic rule, indexed by some keys(s), for secret writing messages into cipher text and secret writing them into plain text. Although standard ways of cryptography can be used to inscribe the pictures however it's prohibited owing to two main reasons:
1 As image size is far larger than that of text, the standard cryptosystems needs more time to directly inscribe the image information.
2. Also, the decrypted text should be equivalent to the initial text, however thanks to the characteristics of human perception the decrypted image mustn't essentially be capable the initial image as tiny distortion in image is suitable as way as human is ready to understand that distortion.
The major components of cryptography are:-

A. Plaintext: the initial information or text is termed plaintext.
B. Cipher Text: the initial message modified to a different unclear format using some algorithmic rule is termed Cipher text.
C. Key: a number on which algorithm is based, like the Caesar cipher text uses key no 3.
D. Encryption algorithm: Key is a number using which algorithmic rule is predicated, just like the Caesar cipher text uses key number three.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

E. Decryption algorithm: Needed at receiver's facet for retrieving the initial message that's to vary the cipher text to plaintext.
F. Hashed message Authentication code: In the process copy of the key is added along with data and combination is hashed using a hash function such as SHA 1.Result is then again prep ended with that same key and result is again hashed using that algorithm. At receiver side the receiver creates its own data and compares it with delivered to validate and check for authentication.
G. Digital signature: A digital signature is signature like information added to verify the information sent by client side in encrypted form.

The major types of Cryptographic Techniques are:

A. Secret Key Cryptography (SKC): A Secret key cryptography uses a fixed length, 56-bit key and an efficient algorithm to quickly encrypt and decrypt messages. It can be easily implemented in hardware, making the encryption and decryption process even faster. In general, increasing the key size makes the system more secure.
B. Public Key Cryptography (PKC): Asymmetric key cryptography overcomes the key management problem by using different encryption and decryption key pairs. The encryption key can be made public, provided the decryption key is held only by the party wishing to receive encrypted messages. Anyone can use the public key to encrypt a message, but only the recipient can decrypt it.RSA is a widely used public/private key algorithm.
C. Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information. More specifically, given a message x, if it is computationally infeasible to find a message y not equal to x such that H(x) = H(y) then H is said to be a weakly collision-free hash function. A strongly collision-free hash function H is one for which it is computationally infeasible to find any two messages x and y such that H(x) = H(y).

Because of development of the Internet technology, digital media can be transmitted conveniently over the network. Therefore, messages have to be secretly carried by digital media by using the different techniques. The major concerns for data transmission are:

A. Confidentiality: the knowledge can't be understood by anyone for whom it had been unintentional.
B. Integrity: the knowledge can't be altered in storage or transit between sender and meant receiver while not the alteration being detected.
C. Non-repudiation: The creator/sender of the knowledge cannot deny at a later stage his or her intentions within the creation or transmission of the knowledge.
D. Authentication: The sender and receiver will make sure every other's identity and therefore the origin/destination of the knowledge.

The major objective of the project is to provide secure transmission through advanced data encryption technique with the concepts pattern generation technique. The data is first encrypted through AES. The encrypted data and key is then converted to patterns using advanced encryption technique. As there is little or no relation between data and key. So it's hard to decrypt by anonymous parties.

II. RELATED WORK

The major advantage of pattern based encryption is that it's difficult to crack, but it's easy to implement [1]. Most hackers exploit the correlation between the cipher and plain text so a new encoding scheme is required such that, though the hacker gets a hint, it should be difficult for him to crack. The image pattern methodology increases the data security to great extent. In this methodology the carrier image is generated by employing a distinctive code known as four out of eight-code and addition of carrier image to original image that result into the encrypted image [2] .The four to eight digit code is also venerable, so rather than encrypting an image in its original pattern, this paper provides another approach within which image is split into totally different elements so that it merged in to a pattern which is solely known to authorized parties. A data encryption algorithm would not be of much use if it is secure enough but slow in performance [3]. The four of the popular secret key encryption algorithms, i.e., DES, 3DES, AES (Rijndael) and Blowfish algorithm has been implemented and performance has been compared. After experiment it is shown that Blowfish is most efficient algorithm. Information security plays an important role in data communication. Any loss to sensitive data can prove to be great loss to the organization [4]. Encryption algorithm plays main role when confidential data is transmitted over the network. The encryption algorithms consume a significant amount of computing resources such as memory, battery power, and CPU time. The correlation between the plain-text and the cipher-text can be

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

exploited by the attackers to deduce the encryption key or, directly, the original data. Key Selection [5] in public key cryptography is a selection process in which keys can be categorized on the basis of their fitness, making GA a good candidate for key generation. Traditional symmetric and asymmetric methods [6]are not suitable when the needed level of security is high. Hash function based systems are although better than traditional methods but are still inadequate in many cases due to their algorithmic complexity as they need the invertible functions to generate hashes which are time consuming and complex.

III.METHODOLOGY

AES is rather sequential in nature because each successive round depends on the output of the prior round. The major modifications done in improving the efficiency of encryption are-Instead of speeding up AES encryption itself, text is being encrypted in the blocks in parallel. Being able to do this will result in huge gains in efficiency and speedup. The parallelization is obtained by

A. Assigning a copy of the entire data
B. The data, split into 128-bit blocks
C. Each block is then encrypted to produce cipher text blocks each block is encrypted in parallel, but the blocks themselves are encrypted sequentially.
D. Data is retrieved by root and cipher text is written to output.

Basic workflow for non-parallel encryption on client side is as follows:

A. Select and extract data from text file.
B. Perform encryption for completely extracted data using AES.
C. Generate symbol pattern for Key.
D. Generate symbol pattern for cipher data.
E. Send the data to server.

Basic workflow for parallel encryption on client side is as follows:

A. Select and extract data from text file.
B. Divide the file data into smaller blocks of equal length.
C. Perform encryption for on each smaller block using AES in parallel.
D. Generate symbol pattern for Key.
E. Generate symbol pattern for cipher data.
F. Send the data to server.

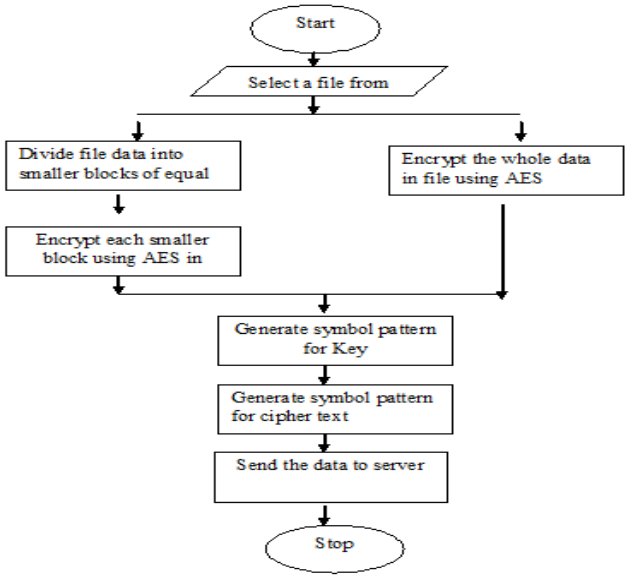

Figure: Encryption process on client side

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Basic workflow for non-parallel encryption on Server Side is as follows:

A. Receive encrypted data and key in symbolic form
B. Extract key from symbolic form.
C. Extract encrypted data from symbolic form.
D. Perform decryption for completely extracted data using AES.
E. Divide the file data into smaller blocks of equal length.
F. Perform encryption for on each smaller block using AES in parallel.

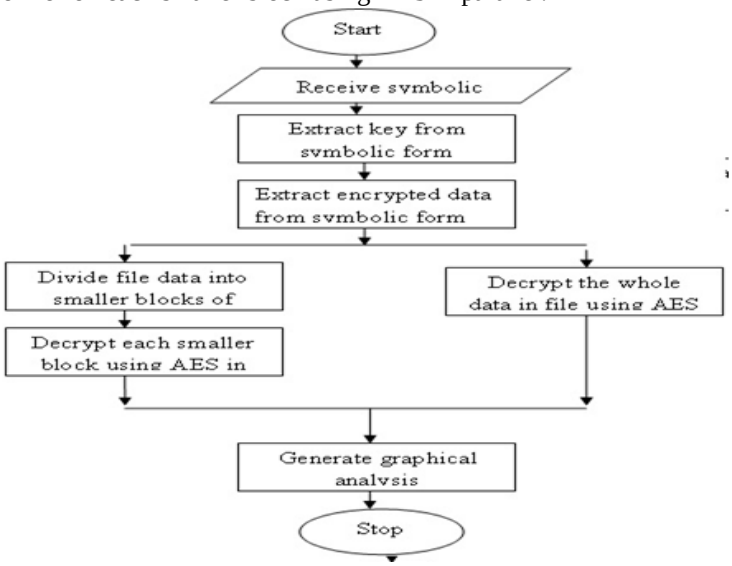

Figure: Decryption process on server side

IV.EXPERIMENTAL RESULTS

Analysis is conducted for the elapsed time for encrypting the file for both algorithms, and then graphical Bar chart isgenerated for comparison. The below comparison result is based on the encryption process of File (.txt) of maximum size 5KB.

Length	AES	Imp AES
4.00 Kb	450 (in milliseconds)	16 (in milliseconds)

Table: Execution time of AES and Imp AES

.

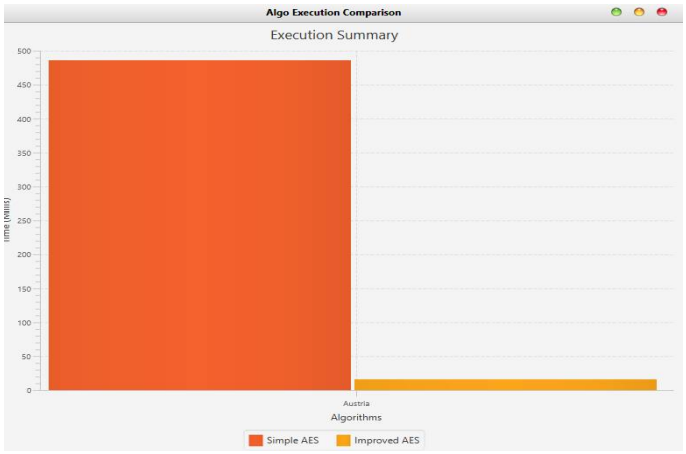

Figure: First analysis of execution time of AES and Imp AES

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

The below table and figure depicts the execution time in millisecond of file size 8 Kb of AES Encryption & Improved AES Encryption.

Length	AES	Imp AES
8.00 Kb	1279 (in milliseconds)	1077(in milliseconds)

Table: Execution time of AES and Imp AES

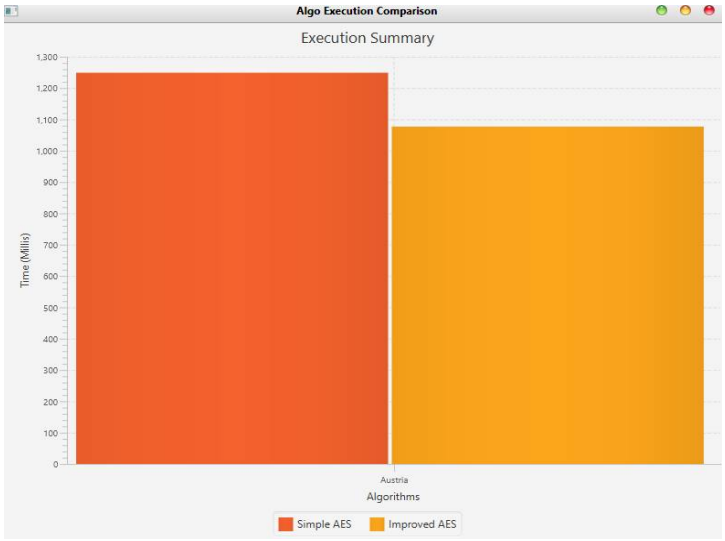

Figure: Second analysis of execution time of AES and Imp AES

V.CONCLUSION

In this paper, the concept of symbol pattern generation and its possibilities of integration with encryption techniques have been explored. Also, an efficient approach of using parallel execution concept in the process of encryption and decryption without using multiple parallel processors and by using only multiple smaller blocks of data have been discussed. The experiments allow us to confirm that, for the AES block cipher and similar algorithms, it is possible to efficiently use the symbol pattern generation for securing AES. Overall, it is concluded that symbol patterns provide an efficient and reliable way to implement AES. The use of parallel encryption decryption concept has greatly improved the efficiency of encryption decryption also. The proposed approach is secure as the cipher text and key will be exposed to another round of encryption i.e. the pattern based encryption and there is little or no relation between the symbolic key and symbolic Cipher text it's hard for hackers to decipher the text by finding a relation between key and cipher text. In the end an analysis of Computational time by the algorithm for same input is shown in a tabular or graphical format on files of different sizes.

There are many possibilities in the increasing security and efficiency of AES encryption in future which includes fully pipelined FPGA implementation of AES Encryption and Decryption

REFERENCES

1. Aamir. (2015). New Cryptographic Techniques For Enhancing Security. International Journal of Scientific & Engineering Research.
2. Bhanot, R. (2015). A Review & Comparative Analysis of Various Encryption Algorithms. International Journal of Security & its Applicartions
3. Efficient Implementation of AES. (2013). International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7 .
4. Gertz, M. (2004). Databases that tell the Truth: Authentic Data Publication. IEEE (volume: 16, Issue: 10).
5. Golle, P. (2004). Secure conjunctive keyword search over encrypted data. proc.,pp. 31-45 ACNS .
6. Hacigumus, H. (2002). Executing SQL over Encrypted Data in the Database Service Provider Model.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

7. Hu, L. (2004). Secure Aggregation for Wireless Network. National Science Foundation.
8. Kainth. (2015). A potent approach to enhance security extent of an image during image encryption. IEEE.
9. M.B.Nivethal. (2014). A Comparative Analysis of Cryptography Algorithms. IJIREECE.
10. Nadeem. (2005). A performance Comparison of Data Encryption Algorithms. IEEE.
11. Patil, A. (2013). A Comparative Survey of Symmetric Encryption Techniques For Wireless Devices.
12. Perrig, A. (n.d.). Spins-security protocols for sensor networks.
13. R.Merkle. (1980). Protocol for Public Key Cryptosystem. IEEES&P .
14. Rehman, S. U. (2012). Comparison Based Analysis of Different Cryptographic & Encryption Techniques Using Messages Authentication Code in Wireless Sensor Networks. International Journal of Computer Science Issues,Vol. 9,Issue 1,No 2, .
15. Saraf, K. R. (n.d.). Text & Image Encryption Decryption Using Advance Encryption Standard. International Journal of Emerging Trends & Technology in Computer Science.
16. Scripcariu, L. (2015). A Study of Methods Used to Improve Encryption Algorithms Robustness. IEEE.
17. Shivangi. (2012). A Survey on the Applications of Cryptography. International Journal of Engineering and Technology Volume 2 No. 3 .
18. Upadhay, V. (ISSN-2230-8849). Secure data in wireless sensor network via des. International Journal of Enterprise Computing & Business Systems.
19. Xiaodong, D. (2002). Practical Techniques for Searches on Encrypted Data. IEEE.