Improving the Efficiency and Security of AES Algorithm using Parallel Computation and Symbol Pattern Generation Technique

Nagma Anjum[1] Bhupesh Dewangan[2]
[1]M.Tech. Student [2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]Bhilai (C.G.), India

Abstract— Information security is an important on internet. There are different kinds of information which are business related, academic or user related private data. Illegal access of the information can lead to big losses, so it is important that proper measures should be taken for securing information on internet. Cryptography is a method of storing and sending facts in a particular form so that only those for whom it is intended can read and process it. The word is most often linked with scrambling plain text (ordinary text, sometimes referred to as clear text) into cipher text and then back again to plain text (known as decryption). The most important factors in information security are Security, integrity, non-repudiation, confidentiality, and authentication services. In now days the security of data attracts much attention, especially when these data are stored in memory or send through the communication networks. Many different data encryption methods have been proposed to keep the security of the data. In this paper we propose an improved AES (Advanced Encryption Algorithm) by using the concepts of parallel computation and the quality of encrypted data is further improved by using symbolic pattern generation techniques. The proposed concept is both fast and more secure for encryption, information transmission and decryption.

Key words: Cryptography, Public Key Cryptography, Private Key Cryptography, Advanced Encryption Standard (AES), Parallel Computation, Symbol Pattern Generation

I. INTRODUCTION

Shielding susceptible data is the end goal of almost all IT protection measures. Two well-built point of view for protecting sensitive data are to avoid identity burglary and to defend privacy. The improper disclosure of sensitive data can also cause disobedience and humiliation to students, faculty, and staff, and potentially harm the reputation of the Institute. Some of the important aspects of information security are:

- Data security is crucial to all academic, medical and business operations.
- Create a plan to review your data security status and policies and create routine processes to way in, store and handle the data safely as well as archive unneeded data.
- Keep only the data needed for routine current business. Back up the data to a safe place in the event of loss.

A. Cryptography

Cryptography is the discipline of making communication inarticulate to everyone except the intended receiver(s). It is the cram of methods of sending data in concealed form so that only intended recipients can remove the disguise and read the data. Cryptography offers efficient solution to protect sensitive information in a large number of applications including personal data security, internet security, diplomatic and military communications security, etc. through the processes of encryption/decryption.

B. Components of Cryptography

- Plaintext: The first information or content is called plaintext.
- Cipher Text: The first message changed to another mixed up arrangement utilizing some calculation is called Cipher content.
- Key: Key is a number on which calculation is based, similar to the Caesar figure content uses key no 3.
- Encryption calculation: This calculation is required next to sender for changing the first message (Plaintext) to unintelligible arrangement (Cipher content) to shield the information from other non substantial recipients.
- Decryption calculation: Required next to receiver for recovering the first message that is to change the figure content to plaintext.
- Hashed message Authentication code: For this situation the duplicate of the key is included alongside information and blend is hashed utilizing the key less hash capacity, for example, SHA 1.Result of this Is HMAC which is on the other hand prep finished with that same key and result is again hashed utilizing that calculation. At beneficiary side the collector makes its own HMAC and contrasts it and conveyed to accept and check for confirmation.
- Digital signature: Like if there should be an occurrence of banks when you sign a Check, they check your mark for validation to see that the client is legitimate. To comprehend the idea of Digital mark, let us take a case there are two clients A and B.A send message to B and B watches that the message originated from A not any other individual. B can request that A sign the message with the goal that it can be demonstrated that A is the real sender and B confirms the realness. This is known as advanced mark.

C. Parallel Computation

Parallel computation is a method in which several computations can be carried out all together on two or more microprocessors. Parallel computation can be performed by parallelizing the execution of algorithm using multi-core and multiprocessor computers having multiple processing elements within a single machine.

II. RELATED WORK

- It is vital to scale back the correlation between the initial message and therefore the encoded version of it victimization enlarged information structures for block

cryptography algorithmic program, longer cryptography key sequences and non-linear operations [1].

- The major advantage of pattern primarily based cryptography is that it's troublesome to crack, however it's straightforward to implement [2]. Most hackers utilize the parallel between the cipher and plain text thus an alternate encryption theme is needed specified, although the eve gets a touch, it ought to be troublesome for him to split.
- The image pattern methodology will increase the information security to nice extent. The carrier image is generated by using a particular code called four to eight figure cipher and addition of carrier image to original image that result into the encrypted image [3] .The four to eight figure cipher is additionally venerable, thus instead of encrypting a picture in its original pattern, this paper provides another approach among that image is split into completely totally different parts so it united in to a pattern that is only proverbial to licensed parties.
- A encryption algorithmic program wouldn't be of abundant use if it's protected enough however slow in routine [4]. The four of the popular secret key cryptography algorithms, i.e., DES, 3DES, AES (Rijndael) and Blowfish algorithmic program has been enforced and performance has been compared. when experiment it's shown that Blowfish is most effective algorithmic program.
- Information security plays a very important role in electronic communication. Any loss to sensitive information will sway be nice loss to the organization [5]. Cryptography algorithmic program plays main role once confidential information is transmitted over the network. The cryptography algorithms consume a big quantity of computing resources like memory, battery power, and processor time.

III. PROBLEM IDENTIFICATION

With the 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, and then be transmitted through the Internet rapidly. The major concerns for data transmission are:

- Confidentiality: The information cannot be understood by anyone for whom it was unintended.
- Integrity: The information cannot be altered in storage or transit between sender and intended receiver without the modification being detected.
- Non-repudiation: The creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.
- Authentication: The sender and receiver can confirm each other's identity and the origin/destination of the information.
- Fast Computation: One of the major issues with encryption algorithms is that the more secure the algorithm is the greater is the execution time. The major objective of the project is to provide secure encryption through advanced data encryption technique with the concepts pattern generation technique. The data is first encrypted through ASA. 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. Also due to parallel execution the execution time is also much lesser.

IV. PROPOSED METHODOLOGY

By proposed procedure the significant steps included in parallel calculation of AES calculation are:

- Store the plaintext and key in a memory space.
- Plain content is isolated in squares of 16 bytes each and each of the pieces is encoded totally in parallel.
- After the encryption of every piece these squares are combined and a last scrambled yield is created.

Essential work process is as per the following:

- Enter plain content.
- Divide the plain content into different pieces.
- Perform encryption utilizing AES calculation of every square utilizing parallel computational idea.
- Generate image design for Key.
- Generate image design for figure information.
- Save the yield.

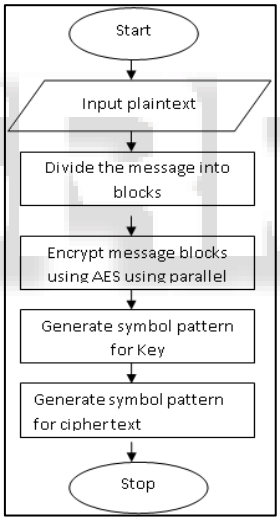

Fig. 1: Flowchart Hybrid Encryption

V. RESULTS AND DISCUSSION

The comparative analysis of running time among the algorithms is as given below.

	AES	HYBRID AES
Time	1936	284

Table 1: Execution time

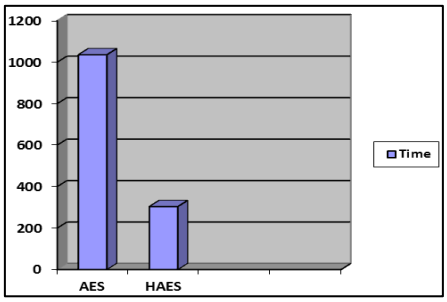

Fig. 1: Execution Time

The above execution time reading clearly shows that the proposed approach has less execution time as compared to traditional Apriori algorithm.

VI. CONCLUSION

In today's scenario one of the major requirements is to use effective techniques in order to protect data from unauthorized access if an attacker somehow manages to steal the data. The work is focused upon improving the security of AES as well as improving its execution time by using the concept of parallel computation.

REFERENCES

[1] "A Study Of Methods Used To Improve Encryption Algorithms Robustness", Scripcariu, L., IEEE 2015.
[2] "New Cryptographic Technique For Enhancing Security", Aamir Mohammed Suhail , Anuraag Vyas, Meghana Gudivada, Prof.T.Venkat Narayana Rao, International Journal of Scientific & Engineering Research,2015.
[3] A potent approach to enhance security extent of an image during image encryption, Kainth, K.IEEE,2015
[4] "A Performance Comparison of Data Encryption Algorithms" Nadeem, A., Javed, M.Y. IEEE, 2005.
[5] "A Comparative Survey Of Symmetric Encryption Techniques For Wireless Devices",Anjali Patil, Rajeshwari Goudar ,August , 2013.
[6] "A Review and Comparative Analysis of Various Encryption Algorithms",Rajdeep Bhanot and Rahul Hans,International Journal of Security and Its Applications, 2015.
[7] "A Comparative Analysis of Cryptography Algorithms", M.B.Nivetha1 Mr.S.Sivaramakrishnan, IJIREECE, 2014
[8] "A Survey on the Applications of Cryptography", Shivangi Goyal University School Of Information ,(International Journal of Engineering and Technology Volume 2 No. 3, March, 2012
[9] "Text and Image Encryption Decryption Using Advanced Encryption Standard", Kundankumar Rameshwar Saraf , Vishal Prakash Jagtap , Amit Kumar Mishra, International Journal of Emerging Trends & Technologand y in Computer Science (IJETTCS)
[10] "Efficient Implementation of AES", «International Journal of Advanced Research in Computer Science and Software Engineering", Volume 3, Issue 7, July 2013.

