International Journal of Advance Research in Engineering, Science & Technology(IJAREST),
ISSN(O):2393-9877, ISSN(P): 2394-2444,
Volume 2, Issue 12, December-2015, Impact Factor: 2.125

ENHANCED AES FOR TEXT ENCRYPTION USING TIMESTAMP (2D)

Mrs Urmila Biradar, Harshada Makhamale, Nainisha Mahindrakar, Rangoli Agarwal, Saurabh Pachauli.
Dept. of computer science engineering, Savitribai Phule Pune university.
G.H.R.C.E.M, Wagholi, Pune, Maharashtra, India.

Abstract: *The project aims at strengthening the AES algorithm further, by using another dimension for enhancing the encryption technique. A generation of time stamp is introduced for every transaction, which shall work as an additional level of security. Since the exact time stamp will only be known to the user, the encryption becomes safer. The introduction of the time stamp also makes the algorithm asymmetric in nature, a definite up from the symmetric nature. Further- more, an additional, selective key method is introduced, in which, the user is asked to select any three alpha-numeric values of his choice, which shall never be used in the key generation. If any such value is generated in the key, the key shall be further modified to suit the user's preference. If an intruder, tries to break the encryption and uses the aforementioned values in the key, an intrusion detection system will be activated, and the owner will be notified. And to neglect the chances of relative key attack, only the 128 bit AES is being used, which will further strengthen the system.*

Index Terms—*Encryption, Decryption, Time stamp, AES.*

I. INTRODUCTION

The rapid change in technologies and increase in data intrusion has led to the development of different encryption algorithms. A new text based encryption technique that uses the advanced encryption algorithm that provides high level security against any intrusion in the transmission of emails or any other message is proposed in this paper. Any data that is to be transmitted in the form of texts can be secured from intrusion. Proposed method is based on AES. AES is a symmetric key algorithm i.e. the public and the private keys are same. In the system proposed in the paper, asymmetric key algorithm will be used. In the asymmetric key algorithm both public key and the private key are different. This method is a 2D based approach. This uses time and space as two dimensions. In the proposed system time stamp is used for enhancing the AES. A timestamp will be generated for every key-stroke (space bar) event. Also, the cipher key length has been reduced to 128 bits as 256 and 192 bits are more prone to relative attacks.

The proposed idea will reduce the file size leading to the faster transmission of data within seconds without compromising the information and security. The intrusion detection is also included in the system. User selective alpha numeric letters from the key are removed for added security.

II. LITERATURE SURVEY

In a review of the IJSER journal, Dr. Mohan has stressed on the importance of the data security. They worked upon enhancing the diffusion power of the AES algorithm. The security of data has now been one of the most important issue. The data needs to be totally secured. The study was too time taking i.e, the process of encrypting and decrypting takes a very long time and thus results in the slow processing of the data security.

The study by Neils Provos and Peter Honeyman also highlighted that the data security only uses the image to hide the data. They had used the Discrete Cosine transform algorithm. The encryption process takes place in such a way that the whole lot of data is shuffled behind an image. The encryption key and the decryption key remains the same, thus making it more prone to the attacks. The data security is low and the data transmission speed is very low due to the large file size. The steganography concept is prone to the relative key attack in which because of the same encryption and decryption key, the data leakage is higher.

The research papers that are published in referred journals during last decade (like Optimized DES using XNOR, Rijndael algorithm through key multiplication, Hide and seek: an introduction to steganography, AES and its functions, etc.) shows that the data security is essential for the fields like personal data use, organizational purpose, military and defence, etc. The major findings in the earlier research are that the data which is being secured uses the image concept with the large key lengths for the encryption as well as the decryption.

Mr. Malik designed crypt21 in his study, a block of cipher which uses the classical substitution whereas a new transposition scheme. The transposition scheme proposed is entirely dependent on key and induces security by having substitution and transposition both dependent on key. The design is iterative and can be extended to many rounds. Strengths include that it is safe from frequency analysis and dependent on original key in many ways. Weaknesses include possibilities of related key attacks due to weak key schedule.

The concept of AES (Advanced Encryption System) algorithm has been used which was symmetric (the encryption key and the decryption key remains same) in nature. In the papers referred to the proposed system, the old traditional concept has the feature of hiding the data behind an image. Due to the presence of the image, the file size for the transmission is comparatively large in size. There are various key lengths used for the encryption and decryption like 128 bits, 192 bits and 256 bits. The 192 bits and 256 bits had been proved more vulnerable to the attacks.

III. PROPOSED SYSYETM

Encryption is the most effective way to achieve data security. In the proposed idea, cipher text is considered as one dimension and the time stamp of the original text is considered as the other, and using a two dimensional mapping technique the encrypted text is converted to a 2D figure.

In the proposed the conventional symmetric encryption is replaced with an asysmetric encryption technique. The “image” from the conventional image based encryption techniques has been removed in the proposed system.

The proposed idea provides us with the high security in the way of selecting any three random alphabets from the cipher text and then whenever the intruder tries to enter the key and if he enters any three of the alphabets, the message will be passed to the user.

The various modules have been designed such as

- Get_time_stamp:- this module will help us to generate the timestamp of each word on a stroke of a spacebar.
- Selective _key:- this module will let the user select the three alphanumeric values , to provide the high security.
- AES:- this module will help in the encryption of the data.
- Rearrange_text:- this module will shuffle the whole text in an editor using the generated timestamp.
- Mailing :- the text data will be mailed after the encryption.
- Intrusion_detection :- a mail will be sent to the user if the intruder tries to intrude the data.The proposed encryption system is asymmetric in nature which provides the different encryption and decryption keys to the users.

The encryption as well as decryption keys both should be known to the intruder in order to decrypt any certain data. The encryption of text will be in such a way that some random figure or pattern will be generated. The traditional concept of steganography includes the hiding of data behind the image leading to the large file size and thus, slower transmission of data takes place. The proposed idea will reduce the file size leading to the faster transmission of data within seconds.

In the proposed idea, 128 bits key length has been used which provides higher security and is more difficult to intrude.

The proposed idea leads to the development of an efficient algorithm in such a way so that each and every attributes get fulfilled successfully. The

algorithm is designed using NetBeans which requires min 1GB RAM, equivalent i3 processor, Windows operating system and JDK.

IV. ARCHITECTURE

Here the architecture shows who the system is going to work:

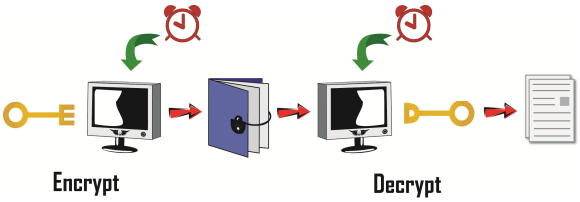

Fig1: Architecture of the system

Clock: Represents the time stamp.
'E' Key: Public key.
'D' Key: Private key.
Locked file: Encrypted text.
Open file: Decrypted text.

V. ALGORITHM

- Cipher(byte in[16], byte out[16], key_arrayround_key[Nr+1])
- begin
- byte state[16]; state = in;
- AddRoundKey(state, round_key[0]);
- for i = 1 to Nr-1 stepsize 1 do
- SubBytes(state);
- ShiftRows(state);
- MixColumns(state);
- AddRoundKey(state, round_key[i]);
- end for SubBytes(state);
- ShiftRows(state);
- AddRoundKey(state, round_key[Nr]);
- End

Algorithm: enhanced AES algorithm

1) Begin.
2) Record time stamp for each space bar key-press event.
3) Associate the previous word with the recorded time stamp.
4) For encryption:
    a. Call AES module.
    b. Retrieve time stamps.
    c. Shuffle the encrypted text using the time stamp.
5) For decryption:
    a. Retrieve time stamps.
    b. Rearrange the text.
    c. Call AES module.
6) End.

Algorithm: rearranging text

1) Begin.
2) Partition the entire screen into "X" parts.
3) Associate each part with a time value (non-sequential, non-random).
4) Compare the time value with the time stamp.
    a. If same, place the text.
    b. If different, find the partition with the same value, and place the text.
5) End.

VI. FUTURE SCOPE AND CONCULSION

The main aim is to create a new encryption technique which uses a small cipher key and provides a higher level of security and to decrease the size of the ciphered text, for faster transmission. To prevent interception and deny message content to the interceptor and to create an asymmetric encryption algorithm.

The proposed idea provides us with high security. Any data that is to be transmitted in the form of texts can be secured from intrusion . The proposed idea will reduce the file size leading to the faster transmission of data within seconds. The use of timestamp makes the encryption more complicated

that makes it almost difficult for the intruders to crack it. The proposed idea can be used in various fields such as the personal data security, corporate data security, military and defense data security and many more. There are various advantages of the proposed idea such as asymmetric key, small size of encrypted file, intrusion detection and many more.

The proposed method is a new method using a 2D space-time based strategy for text encryption. The conventional techniques is extended to using both space and time for encryption. A generation of time stamp is introduced for every transaction, which shall work as an additional level of security. Since the exact time stamp will only be known to the user, the encryption becomes safer. The method is effective and feasible. The proposed method can enhance the security of conventional cryptosystems. It forms a random pattern with the words, hence making it even more difficult to decipher the text.

Thus this method using both time and space as the important attributes increases the security of transmission of any text data.

VII. ACKNOWLEGMENT

We here by wish to take this opportunity to express our gratitude to our teachers and friends and all who have helped toward the completion of our project. We take a great honour in presenting this Project Report to our Principal Prof. D.D.Shah. We also like to give thanks to our H.O.D. Mrs. Poonam Gupta for helping us and guiding us throughout our endeavor.We are very grateful to our Guide Mrs. Urmila Biradar for her guidance through the project. We are very grateful to our teaching staff for guiding us all over the duration of the degree. They were very helpful to us, as and when we required their help. We are also very grateful to non-teaching staff to help us in the laboratory in various ways.

REFERENECES

[1]Niels.xtdnel,nl*/papers/practical.pdf*

[2]*www.ijser.org/paper/improvementsp-of-rijndael--algorithm -through-key-multiplication.html*

[3]Citeseerx,*ist.psu.edu/showciting?cid=180372*

[4]*Research.microsoft.com/en-us/projects/cryptanalysis/aesbc.pdf*

[5]*Crypto.stackexchange.com/related-key-attacks-on-aes.html*

[6] Hyubgun Lee, Kyounghwa Lee, Yongtae Shin, *AES Implementation and Performance Evaluation on 8-bit Microcontrollers, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6 No. 1, 2009.*

[7] Ritu Pahal, Vikas kumar, *International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013*

[8] Julia Juremi Ramlan Mahmod, Salasiah Sulaiman Jazrin Ramli, *Enhancing Advanced Encryption Standard S-Box Generation Based on Round Key , International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): 183-188 The Society of Digital Information and Wireless Communications (SDIWC) 2012 (ISSN: 2305-0012)*