Performance Analysis of SMS security by using Enhanced AES algorithm for mobile phones

Akshay D. Isalkar[1], Shraddha N. Karale[2]
[1]*DMIETR, Wardha, India*
[2]*RGCER, Nagpur, India*

***Abstract*- Message authentication is an important security tool. But, without some security mechanism, it is difficult to send data in secure manner. Most popular shortest and cheapest textual form of communication is short message service (SMS). Cryptography is the one of the main categories of computer security that converts information from its normal form into an unreadable form by using Encryption and Decryption Techniques. To ensure the security of the texts which is sent, many encryption algorithm are available. This paper will focus on message security and to secure the text data while transmitting in the network. The data which is to be transmitted from sender to receiver in the network must be encrypted using the encrypted algorithm.). Symmetric key algorithm reduces the problem of computational overhead and to the calculation of algorithm and improves the performance of encryption. The proposed paper is to provide more efficient authentication mechanisms for textual data. Results show that time taken for various encryption algorithms using our proposed approach is optimized as compared to AES approach.**

***Index Terms*- SMS, Cryptography, AES, Encryption and Decryption.**

I. INTRODUCTION

Apart from electronic chatting, SMS today has become an accustomed source for communicating confidential or proprietary information. When this is the situation the imperative factor is "Security". One commonly used technique to provide security is Encryption [1] Normally a typical text or image has a very large size. Using traditional encryption algorithm will make encryption difficult for large volume of textual data. For the encryption of any textual data we need such algorithms that require less computation because of large size of data. Symmetric-key algorithms are fewer computationally serious than any Asymmetric-key algorithms. Typically, symmetric key algorithms are thousands times sooner than those of the asymmetric algorithms [2]. So the better suitable method to encrypt the textual data is, to encrypt it with symmetric key encryption algorithms. The proposed system use one of the symmetric key algorithm i.e. AES. This is very fast symmetric key algorithm. But in this algorithm due to some restrictions large number of data takes large computation time and encryption speed makes slow.

There are some important terms are used to secure private information.

A. Encryption:

It requires encryption algorithm and key. To encrypt more data, symmetric encryption is used .A symmetric key is used for both the encryption and decryption processes.

B. Decryption

It requires decryption algorithm and key. It is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer are able to read and understand. This method could be used to description of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys.

C. Key

Key is the combination of numeric and alphanumeric text symbols. Key plays an important role in security mechanism like cryptography. Encryption algorithm depends on key.

D. Plain Text

Communication between two sides by using original message is called as Plain Text.

E. Cipher Text

The message which cannot be understood by any unauthenticated person. This cipher text is formed from plain text.

II. SYMMETRIC AND ASYMMETRIC ENCRYPTIONS

There are two main categories of cryptography depending on keys used to encryption and decryption of the data. There are two main categories. They are Asymmetric and Symmetric encryption techniques. AES is one of the most secure algorithm. AES algorithm have four stages Substitution byte, Shiftrows, Mixcolumns and AddroundKey. But AES have some problems like Computation time and Accuracy. To solve these problems we use Enhanced AES. In this algorithm instead of Mixcolumn Step algorithm we use Permutation step. So Enhanced AES is being designed to address the issue related to simple AES and improve the performance of encryption

Our Aim is secure computing by using user access mechanism. In this we provide security to SMS by using AES algorithm to improve the overall performance of AES. And the objectives are:

- SMS security by using Enhanced AES algorithm.
- Performance comparison between some encryption algorithm like DES, RC4 and AES

III. LITERATURE SURVEY

In the research paper [1] proposed the Hybrid Compression encryption technique for securing SMS data. The proposed technique compresses the SMS to reduce its length, then encrypts it using encryption algorithm. Confidential information is exchanged using SMS. So there is need to secure SMS from different threats. The threats are like DoS attack, Message Disclosure, SMS viruses, Phone crashes. Also need to ensure message is send by authorized sender. In order to achieve all these needs this paper describes the solution for SMS security.

Symmetric-key algorithms also known as single- key, one-key and private-key encryption are a class of algorithms for cryptography, that uses a Private(shared secret) key and a Public (non-secret) key to execute encryption or decryption process[2]. The different performance factors are discussed such as key value, computational speed they concluded that AES algorithm is better among Symmetric algorithm. There are two basic types of cryptography: Symmetric Key and Asymmetric Key. Symmetric key algorithms are the quickest and most commonly used type of encryption. Here, a single key is used for both encryption and decryption. There are two basic types of cryptography: Symmetric Key and Asymmetric Key. Symmetric key algorithms are the quickest and most commonly used type of encryption. Here, a single key is used for both encryption and decryption [3]. The survey of SMS encryption as well as decryption techniques, algorithms, models use in communication network and security. Encryption is the process of converting plain text “unhidden” to a cryptic text “hidden” to secure it against data thieves. This process has another part where cryptic text needs to be decrypted on the other end to be understood [4]. The fair comparison between three most common symmetric key algorithms like DES, Blowfish and AES. A comparison has been made on the basis of these Parameters: rounds, block size, key size, encryption/decryption time, CPU process time in the form of throughput and power consumption. These results show that blowfish is more suitable than AES [5]. Various experimental factors are analyzed. Based on the text files used and the experimental result was concluded that DES algorithm consumes least encryption time and AES algorithm use least memory usage, Encryption time differs in case of AES algorithm and DES algorithm [6]. All the techniques are Useful for real-time encryption. Each technique is unique in Its own method, which might be suitable for different applications Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques, will always work out with high rate of security [7]. The Information or SMS security is important problem in network secure communication. Encryption and decryption algorithms uses by many authors for performance evaluation and security. Some algorithms gives better performance but require more time for encryption. The users who uses the AES algorithms. They modified and doing changes in AES algorithm for reducing complexity in the encryption process [8]. Weakness of the Advanced Encryption Standard (AES) provided by the substitution step of

the algorithm, which replaces each input data byte with a fix value provided by a static substitution box (S-box). Efficiently attacks on software programs secured by AES, are concentrated on whitening the S-box, in order to compromise the encryption key and the private information [9]. The different symmetric encryption algorithms like DES, 3DES, AES have been analyzed with respect to different parameters and data types. The Cryptographic process makes use of an algorithm and a secret (key) value. The key can be same for both encryption-decryption process or can be a different one depending on the type of encryption algorithm used. Depending upon the type of key used, cryptography techniques can be divided into two different categories - Symmetric (secret) and Asymmetric (public) key encryption [10]. There are many conventional and symmetric encryption algorithms available to bestow this, each having its own level of security and performance. The most important aspect needed to be considered while using cryptography to provide SMS security is the storage and processing capabilities of the mobile phone which is the main source of the SMS. Considering all aspects this paper proposes a means of providing high authentication and security to the messages shared which can be efficiently used in small devices like mobile phones [11].

A Novel FPGA Implementation of AES-128 using Reduced Residue of Prime Numbers based S-Box. In this paper, we present a novel Field Programmable Gate Array (FPGA) implementation of advanced encryption standard (AES-128) algorithm based on the design of high performance S-Box built using reduced residue of prime numbersThe main motive is to present an efficient hardware usage of AES-128 using Very High Speed Integrated Circuit Hardware Description Language (VHDL). The novel S-Box look up table (LUT) entries forms a set of reduced residue of prime number, which forms a mathematical field. The S-Box with reduced residue of prime number introduces more confusion to the entire procedure of AES algorithm [12]. Original AES algorithm has some advantages in data ciphering area. However, AES suffer from some drawbacks such as high computations, sample in ciphered images, and hardware requirement. Furthermore, those problems are much more complicated when original AES algorithm will use for images ciphering especially for the HD images. Due to these reasons, some modifications are required to boost the performance of AES algorithm in terms of time ciphering and pattern appearance. First modification is reducing the number of rounds to one while the second modification is replacing the S-box with new S-box to decrease the hardware requirements. Applying modified AES in one of the ciphering mode solves the pattern appearance problems. A Survey on Rapid Encryption Method [REM] Derived from AES Algorithm for Grey Scale HD Image Encryption [13].

IV. PROPOSED WORK

Our proposed system develops an application for SMS security on Android Platform. We use Enhanced AES instead of Simple AES algorithm In-order to increase computation speed. Four Stages of Enhanced AES Algorithms are: Substitution bytes , ShiftRows, Permutation (instead of Mixcolumn in simple AES), AddRoundKey.

This system provides a performance comparison between most common encryption algorithms like DES, RC4, and AES (Rijndael).

- In proposed system, first we register all the users.
- Only authenticated users sends the secrete message.
- Proposed system provides encryption.
- On receiver side only authenticate user can have access this secrete message.

V. METHODOLOGY

a. AES Algorithm

The Advanced Encryption Standard (AES) is given by the National Institute of Standards and Technology for the encryption of text. Encryption transforms data to some scrambled form called cipher text while decryption converts the scrambled text back to original form called plaintext. The AES algorithm is based on permutations and substitutions. Permutation creates diffusion in data while substitution creates confusion in data .Steps for Encryption, each round consists of these 4 steps-

- Substitute Bytes

Sub Bytes transformation is a byte substitution using a substitution table named SBox. This substitution operation takes each byte in the State matrix and puts a new byte as per the SBox table [7]. It is a 16 × 16 matrix; the entries in this matrix are created by using multiplicative inverse followed by affine transformation to destroy the bit level correlation in each byte

- Shift rows

This permutation step rotates bytes in the State matrix to the left. Row 0 of is rotated 0 positions to the left, row 1 is rotated 1 position left, row 2 is rotated 2 positions left, and row 3 is rotated 3 positions left [7].

- MixColumn

This substitution operation is responsible for inter-byte diffusion .Each column of state matrix is multiplied with a fixed polynomial matrix [8].

$$\begin{bmatrix}2&3&1&1\\1&2&3&1\\1&1&2&3\\3&1&1&2\end{bmatrix}\begin{bmatrix}S_{0,0}&S_{0,1}&S_{0,2}&S_{0,3}\\S_{1,0}&S_{1,1}&S_{1,2}&S_{1,3}\\S_{2,0}&S_{2,1}&S_{2,2}&S_{2,3}\\S_{3,0}&S_{3,1}&S_{3,2}&S_{3,3}\end{bmatrix}=\begin{bmatrix}S'_{0,0}&S'_{0,1}&S'_{0,2}&S'_{0,3}\\S'_{1,0}&S'_{1,1}&S'_{1,2}&S'_{1,3}\\S'_{2,0}&S'_{2,1}&S'_{2,2}&S'_{2,3}\\S'_{3,0}&S'_{3.1}&S'_{3,2}&S'_{3,3}\end{bmatrix}$$

The MixColumns transformation of a single column j ($0 \le j \le 3$) of state can be expressed as:

$$S'_{0,j} = (2 * S_{0,j}) \oplus (3 * S_{1,j}) \oplus S_{2,j} \oplus S_{3,j}$$
$$S'_{1,j} = S_{0,j} \oplus (2 * S_{1,j}) \oplus (3 * S_{2,j}) \oplus S_{3,j}$$
$$S'_{2,j} = S_{0,j} \oplus S_{1,j} \oplus (2 * S_{2,j}) \oplus (3 * S_{3,j})$$
$$S'_{3,j} = (3 * S_{3,j}) \oplus S_{1,j} \oplus S_{2,j} \oplus (2 * S_{3,j})$$

The InvMixColumns is defined by the following matrix multiplication:

$$\begin{bmatrix}0E&0B&0D&09\\09&0E&0B&0D\\0D&09&0E&0B\\0B&0D&09&0E\end{bmatrix}\begin{bmatrix}S_{0,0}&S_{0,1}&S_{0,2}&S_{0,3}\\S_{1,0}&S_{1,1}&S_{1,2}&S_{1,3}\\S_{2,0}&S_{2,1}&S_{2,2}&S_{2,3}\\S_{3,0}&S_{3,1}&S_{3,2}&S_{3,3}\end{bmatrix}$$
$$=\begin{bmatrix}S'_{0,0}&S'_{0,1}&S'_{0,2}&S'_{0,3}\\S'_{1,0}&S'_{1,1}&S'_{1,2}&S'_{1,3}\\S'_{2,0}&S'_{2,1}&S'_{2,2}&S'_{2,3}\\S'_{3,0}&S'_{3.1}&S'_{3,2}&S'_{3,3}\end{bmatrix}$$

Inverse of the first matrix is shown in second matrix. If we label these A and A−1 respectively and we label state before the mix columns operation as S and after as S', we can see that:

AS = S'

Therefore,

$A^{-1}S' = A^{-1}AS = S$

- The Key Expansion

The AES encryption and decryption algorithms use a key schedule generated from the seed key array of bytes. Multiple keys from an initial keys are used so as to increase the diffusion in bits by some amount. The new keys computed from key expansion are called the round keys, this way they are distinguished from the original key.

b. Enhanced AES

To reduce the problem of high computation and computational overhead we use the AES and modify it. The AES is also known as modified AES because of by totaling the initial permutation step takes from DES in order to enlarge encryption performance. Modified AES has four steps, these four steps are as follows:

- *Substitution Byte*
- *ShiftRow*
- *Permutation*
- *AddRoundKey*

Here we use Permutation instead of MixColumn Substitution Byte, ShiftRow, and AddRoundKey remain same as in AES. Permutation is widely used in cryptographic algorithms. Permutation operations are interesting and important from both cryptographic and architectural points of view. The DES algorithm will provide us permutation tables. The inputs to the IP table consist of 128 bits. Modified-AES algorithm takes 128 bits as input. The functions Substitution Bytes and Shift Rows are also interpreted as 128 bits whereas the Permutation function also takes 128 bits. In the permutation table each entry indicates a specific position of a numbered input bit may also consist of 256 bits in the output. While reading the table from left to right and then from top to bottom, we observe that the 242th bit of the 256-bit block is in first position, the 226th is in second position and so forth. After applying permutation on 128 bits we again complete set of 128 bits and then perform next remaining functions of algorithm. If we take the inverse permutation it gives again the original bits, the output result is a 128-bit cipher text. For the full decryption of Modified-AES algorithm the transformation processes are, Inv-Bytesub, Inv-Shiftrows, Inv-Permutation, and the Addroundkey, which are performed in 10 rounds as it is in the encryption process[20].

Substitution Bytes, ShiftRows and AddRoundKey remain unaffected as it is in the AES. Here the important function is Permutation which is used instead of Mixcolumn.

VI. EXPERIMENTAL ENVIRONMENT

The hardware platform in this project uses a PC with the configuration: I3processor, 2 GB RAM and 2 GB hard disk. The software environment uses the following configuration: Android operating system, SDK and Eclipse, Netbeans ; JAVA are used as a programming language. Android SDK, ADT Plugin, Some Android SDK packages, USB drivers.SQL-Lite as a Database

VII. RESULTS

For testing the algorithm we use a very simple code that checks the efficiency of algorithm. This test shows that the Enhanced AES algorithm is much better than other encryption algorithm like DES and RC4 time of both the Enhanced AES with and other encryption algorithm

Table1: Computational Time between Algorithms

Algorithm	AES	DES	RC4
Time (ms)	4	18	16

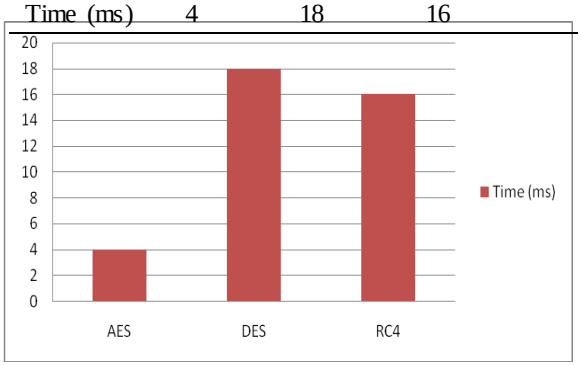

Fig 1: Comparison graph between Encryption Algorithm

VIII. CONCLUSION

As the size of text increases the efficiency of simple AES algorithm decreases. The time complexity is depends on encryption type. To overcome the difficulties, we have proposed Enhanced AES algorithm that uses permutation instead of MixColumn on to reduce time taken for encrypting data and to provide more security to the data.

Results have shown that time taken for encryption using our proposed approach is optimized as compared to other encryption algorithm Usually lightweight encryption algorithms are very attractive.. For the security of textual data, we have proposed an encryption algorithm that is based on AES using symmetric key encryption algorithm. In version of security analysis and experimental results our proposed encryption scheme is fast.

Future Scope

The work have been till done in this thesis is a good beginning of research on how to used AES for providing security to SMS enhances the performance of AES algorithm. Even though our research is limited by the time and environment, some meaningful results have been got. This thesis only contains the finished parts of the research.

In future we can perform same experiments on image data, audio data & video data and developing a stronger encryption technique with high speed and for great throughput.

REFERENCES

[1] Sri Rangarajan, N. Sai Ram, N. Vamshi Krishna , “Securing SMS using Cryptography”, (IJCSIT) Vol. 4 (2) 2013,285 -288

[2] Pravin Kawle, Avinash Hiwase, “Modified advanced encryption standard”, (IJSCE)

[3] Sunita B. , Anita B., S.K.Sharma ,“A new Approach towards Encryption Schemes: Byte-Rotation Encryption Algorithm”, World CECS 2012

[4] Basel Alomair,, Senthilnathan Muthukumaravel , “Efficient Authentication For Mobile and Pervasive Computing IEEE transactions on mobile computing”, - MARCH 2014

[5] Oyshee Brotee Sahoo, Dipak K Kole, Hafizur Rahaman, “An Optimized S-Box for Advanced Encryption Standard(AES) Design”, International Conference on Advances in Computing and Communications, ©2012 IEEE

[6] Niharika Tyagi, Priyanka, “A Survey on Ensemble of Modifications on AES Algorithm”, Journal of Basic and Applied Engineering Research Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 1, Number 7; October, 2014 pp. 19-24

[7] Rais, M., H., Qasim., S., M. A, " Novel FPGA Implementation of AES-128 using Reduced Residue of Prim e Numbers based S-Box", International Journal of Computer Science and Network Security, 2009, 9, 9, p. 5

[8] Julia Juremi, Ramlal Mahmod, Salasiah Suleman, JazrinRamli, "Enhancing Advanced Encryption Standard S-Box Generation Based On Round Key", (IJCSDF)1(3):18 188(SDIWC)2012(ISSN:2305-0012).

[9] Basel Alomair and Radha Poovendran, "E-MACs: Towards More Secure and More Efficient Constructions of Secure Channels",

[10] Poonam Mandavkar, Gauri Patil, Chetna Shetty, "SMS Security for Android Mobile Using Combine Cryptographic Algorithms", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 4, April 2014

[11] Basel Almair, "Authenticated Encryption: How Reordering can Impact Performance", ACNS'12 Proceedings of the 10th international conference on Applied Cryptography and Network Security, 2012

[12] Jawahar Thakur, Nages Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithm Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering December 2011

[13] B. Padmavathi, , S. Ranjitha Kumari, "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique" , - IJSR,April-2014

[14] Punam V. Maitri, Rekha V. Sarawade, "MSC: Mobile Secure Communication Using SMS in Network Security: A Survey", - International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 11, November - 2013

[15] Kawle, Avinash Hiwase, Gautam Bagde, "Modified Advanced Encryption Standard", Pravin (IJSCE)-April 2013

[16] Jigar Chauhan, Neekhil Dedhia, "Enhancing Data Security by using Hybrid Cryptographic Algorithm", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 3, May 2013

[17] Nidhi Singhal , J.P.S.Raina , "Comparative Analysis of AES and RC4 Algorithms for Better Utilization" IJCTTE- August 2011

[18] Md Asif Mushtaque, "Comparative Analysis on Different parameters of Encryption Algorithms for Information", JCSE-April-2014

[19] Jawahar Thakur, Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", IJETAE- Dec-2011

[20] Shraddha Karale, Prof. Kalyani Pendke, Prof.Prashant Dahiwale , "The Survey of Various Techniques & Algorithms for SMS Security", ,IEEE ICIIECS'15

[21] G. Ramesh and R. Umarani, "Data Security In Local Area Network Based On Fast EncryptionAlgorithm", - ICTACT-June 2010

[22] Nidhi Singha, J.P.S.Raina, "Comparative Analysis of AES and RC4 Algorithms for Better Utilization", - IJCT-2011

[23] L. Scripcariu and P. D. Mătăsaru, "On the substitution method of the AES algorithm," International Symposium on Signals, Circuits and Systems ISSCS2013, Iasi, 2013, pp. 1-4. doi: 10.1109/ISSCS.2013.6651172