A More Effective Approach Securing Text Data Based On Private Key Cryptography

Ekta Agrawal
Research Scholar, Faculty of Computer Science
Pacific Academy of Higher Education & Research University
Udaipur, Rajasthan, India
e-mail:ektaagrawal4jan@gmail.com

Dr. Parashu Ram Pal
Professor, MCA
Lakshmi Narain College of Technology,
Bhopal, M.P., India
e-mail: prpal@rediffmail.com

Abstract **-** Internet & smart phone makes easy to access and share data from anywhere in the world. Every day terabytes of data are being generated and used. Several important real life applications like banking transactions, credit information, and confidential data is transferred using internet. All the users need to prevent their data from unauthorized access. Data security during communication using internet and smart phone is a difficult task. Cryptography plays an integral part in data security. Cryptography provides confidentiality and maintains integrity between genuine users. Cryptography used mathematical techniques for security aspects such as confidentiality, data integrity, entity authentication, and data authentication. A cryptographic algorithm works using combination of keys to encrypt the plaintext. The security of encrypted data is entirely dependent on the strength of the cryptographic algorithm and the secrecy of the key. In this paper an efficient approach based on private key to encrypt and decrypt text data is proposed.

Keywords: *Encryption, Decryption, Symmetric Key Cryptography, Asymmetric Key Cryptography.*

*****

I. INTRODUCTION

There are several different encryption techniques are used to protect the confidential data from unauthorized use. The evolution of encryption is moving towards a future of endless possibilities. Every day new methods of encryption techniques are developed. The six main important factors that have to be considered for method are shown in Figure 1. They are as follows:

1. Confidentiality: Confidentiality specifies that only the specified sender and receiver should be able to access the contents of a data.

2. Authentication: It is mechanisms to establish proof of identities. This process ensures that the origin of the data is correctly identified.

3. Integrity: It ensures that the contents of the data remain the same when it reaches the recipient.

4. Non- repudiation: Non-repudiation does not allow the sender of a message to refute the claim of not sending the message.

5. Access Control: Access Control specifies and controls who can access what.

6. Availability: The principle of availability states that resources should be available to authorized parties all the times.

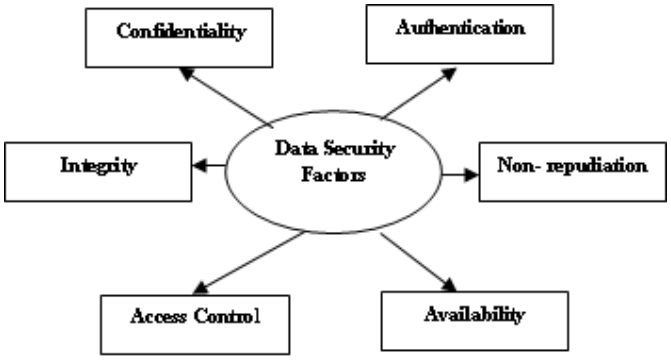

Figure 1 Data Security factors

II. TYPES OF ENCRYPTION TECHNIQUES

There are two main ways to do encryption today. The first kind of encryption, called symmetric cryptography or shared secret encryption and second is called public key encryption (PKE), also known as asymmetric cryptography.

A. Private Key Cryptography or Symmetric Cryptography

This form of encryption uses a secret key, called the shared secret, to scramble the data into unintelligible gibberish. The person on the other end needs the shared secret (key) to unlock the data the encryption algorithm. User can change the key and change the results of the encryption. It is called symmetric cryptography because the same key is used on both ends for both encryption and decryption. The encryption

 ISSN: 2321-8169
163 – 168

and decryption process used by the sender and receiver in symmetric key cryptography is shown in Figure 2.

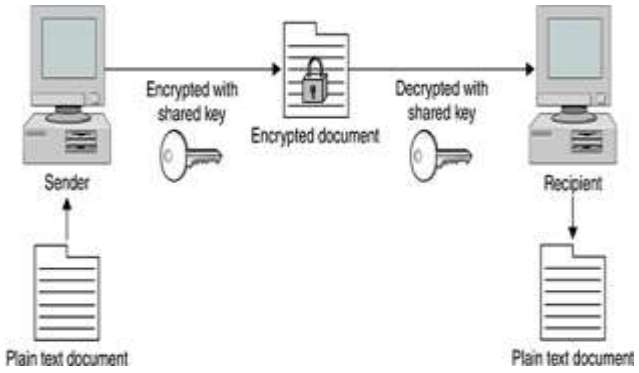

Figure 2 Symmetric Cryptography

The problem with this method is that user has to communicate the secret key securely to the intended recipient. If any unauthorized user intercepts the key, the message can be read by the unauthorized user.

2.2 Public Key Encryption (PKE) or Asymmetric Cryptography

Asymmetric Cryptography uses encryption that splits the key into two smaller keys. One of the key is kept as public and another is kept private. User encrypts a message with the recipient's public key. The recipient can then decrypt it with their private key. They can do the same for you, encrypting a message with your public key so you can decrypt it with your private key. The difference here is that user don't need someone's private key to send him or her secure message. By using recipient's public key, you know that only that person can encrypt it using his or her private key. This system allows two entities to communicate securely without any prior exchange of keys. Figure 3 shows the working of Asymmetric Key Cryptography.

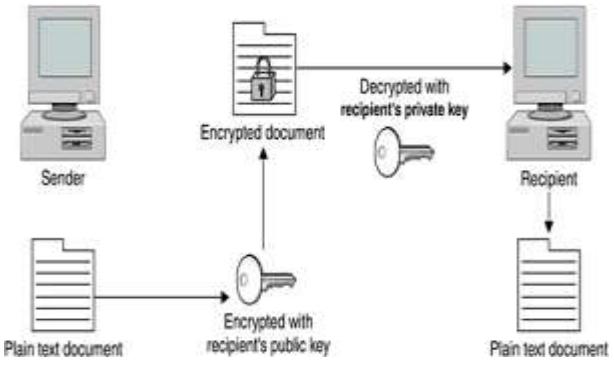

Figure 3 Asymmetric Cryptography

Symmetric cryptography is usually implemented by the use of one-way functions. In mathematic terms, these are functions that are easy to compute in one direction but very difficult to compute in reverse. This is what allows you to publish your public key, which is derived from your private key. It is very difficult to work backwards and determine the private key. A common one-way function used today is factoring large prime numbers. It is easy to multiply two prime numbers together and get a product. However, to determine which of the many possibilities are the two factors of the product is one of the great mathematical problems. If anyone were to invent a method for easily deducing factors of large prime numbers, it could make obsolete much of the public key encryption used today.

III. SECURITY ARCHITECTURE

The architecture for security is shown in Figure 4.

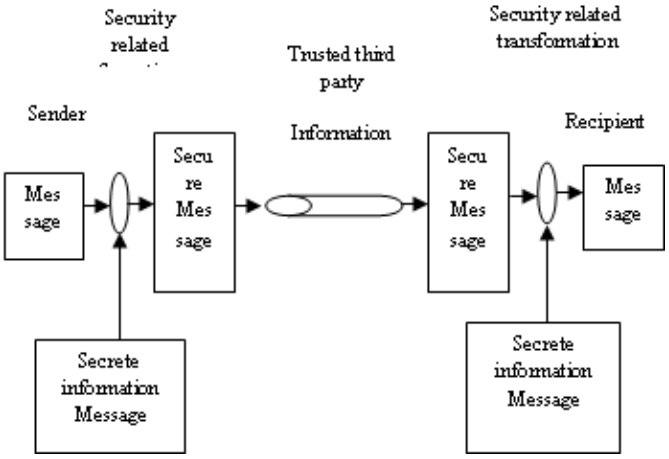

Figure 4 Security Architecture

A message is to be transferred from one party to another across some sort of internet. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

IV. LITERATURE REVIEW

Several papers have been reviewed and observed certain aspects to implement the effective approach for encryption and decryption algorithm for security.

In 2010 Ayushi proposed "A Symmetric Key Cryptographic 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 few well-known symmetric key algorithms i.e. DES, RC2, RC4, IDEA etc. She represents various symmetric key algorithms in detail and then proposes a new symmetric key algorithm. Algorithms for both

encryption and decryption are provided here. The advantages of this new algorithm over the others are also explained. [4]

In 2011 Vinod Shokeen, Niranjan Yadav proposed "Encryption and Decryption Technique for Message Communication". They proposed a fast and secure encryption algorithm using substitution mapping, translation and transposing operations. The proposed symmetric encryption technique has two advantages over traditional schemes. First, the encryption and decryption procedures are much simpler, and consequently, much faster. Second, the security level is higher due to the inherent poly-alphabetic nature of the substitution mapping method used here, together with the translation and transposition operations. [5]

In 2011 B. Ravi Kumar, Dr. P. R. K. Murti proposed "Data Encryption and Decryption process Using Bit Shifting and Stuffing (BSS)". Bit Shifting and Stuffing (BSS) represent only seven bits per its ASCII value. In computer system to represent a printable character it requires one byte, i.e. 8 bits. So a printable character occupies 7 bits and the last bit value is 0 which is not useful for the character. In BSS method we are stuffing a new bit in the place of unused bit which is shifting from another printable character. So in this BSS methodology after encryption, for every eight bytes of plain text it will generate seven bytes cipher text and in decryption, for every seven bytes of cipher text it will reproduce eight bytes of plaintext. [6]

In 2012 Ch. Santhosh Reddy, Ch. Sowjanya, P. Praveen, proposed "Poly-alphabetic Symmetric Key Algorithm Using Randomized Prime Numbers". They discussed types of cryptography and different keys in cryptography. They give brief description about symmetric key algorithms and we are proposing new algorithm in symmetric key cryptography. They proposed a algorithm which contains two levels of Exclusive OR (XOR) operation. Proposed algorithm is useful in transmission of messages and data between one user and another. [7]

In 2012 Monika Agrawal & Pradeep Mishra proposed "Comparative Survey on Symmetric Key Encryption Techniques". They present a detailed study of most of the symmetric encryption techniques with their advantages and limitations over each other. [8]

In 2013 Krishna Kumar Pandey & Vikas Rangari proposed "An Enhanced Symmetric Key Cryptography Algorithm to Improve Data Security" Proposed work used enhanced symmetric key encryption algorithm, in which same structure of encryption and decryption procedure algorithm is used. The proposed algorithm uses key generation method by random number in algorithm for increasing efficiency of algorithm. This algorithm use key size of 512 bits for providing better security and it also provide the concept of internal key generation at receiver end on the basis of 512 bits key which will entered by the sender. [9]

In 2013 Obaida Mohammad & Awad Al-Hazaimeh proposed "A New Approach for Complex Encrypting and Decrypting Data". They enhanced security goals by using maintains of the communication channels by making it difficult for attacker to predicate a pattern as well as speed of the encryption / decryption scheme. [10]

In 2014 Ezeo for C. J. & Ulasi A. G proposed "Analysis of Network Data Encryption & Decryption Techniques in Communication Systems" They present analysis of network data encryption and decryption techniques used in communication systems. Visual Basic simulation program that encrypt and decrypt data were developed, written and tested. Different data block sizes were captured and plotted against total time response taken during data encryption using Microsoft Excel. [16]

In 2014 Satyajeet R. Shinge & Rahul Patil proposed "An Encryption Algorithm Based on ASCII Value of Data". They presented a symmetric cryptographic algorithm for data encryption and decryption based on ASCII values of characters in the plaintext. The proposed algorithm encrypts the plaintext using their ASCII values. The secret key is converted to another string and that string is used as a key to encrypt or decrypt the data. [17]

In 2014 Mitali & Vijay Kumar proposed "A Survey on Various Cryptography Techniques" This represented a fair performance comparison between the various cryptography algorithms on different settings of data packets. They analyze the encryption and decryption time of various algorithms on different settings of data. [18]

In 2015 Suchita Tayde & Seema Siledar proposed "File Encryption, Decryption Using AES Algorithm in Android". They used Advanced Encryption Standard and implemented on various platforms especially in small devices like mobile phone. Proposed application allows user to run application on android platform to encrypt the file before it is transmitted over the network. It is used for all type of file encryption such as text, docx, pdf and image encryption. [19]

In 2015 Zaeniah, Bambang Eka Purnama proposed "An Analysis of Encryption and encryption Application by using One Time Pad Algorithm ".Security of data in a computer is needed to protect critical data and information from other parties. One way to protect data is to apply the science of cryptography to perform data encryption. There is wide

variety of algorithms used for encryption of data; this study used a one-time pad algorithm for encrypting data. Algorithm One Time Pad uses the same key in the encryption process and a decryption of the data. An encrypted data will be transformed into cipher text so that the only person who has the key can open that data. Therefore, analysis will be done for an application that implements a one-time pad algorithm for encrypting data. The application that implements the one time pad algorithm can help users to store data securely. [20]

V. PROBLEM STATEMENT

Several methods have been developed for encrypting and decrypting but each and every method has some advantage and disadvantage. The main problem is

A. Complex calculation: - Each and every approach used mathematical calculation, complex calculation need more time for encryption and decryption.

B. Number of keys: -Number of key used to encrypt the data is an important factor. Number of keys key should be effective and minimum.

C. Key Size: -Private Key based algorithm used common key shared by sender and receiver. These key are decided by the sender and same key is used by receiver. The length of the key should me minimum is size.

VI. PROPOSED ALGORITHM

The steps followed in the proposed encryption algorithm are as follows:

Step 1. Assign number to alphabets from 1 to 26.

Step 2. Suppose L is the size of text string.

Step 3. If L is divisible by two, then key is L/2 Else Key should be (L+1)/2

Step 4. Now used formula (alphabets number + key value) modulus 26.

Step 5. Now replace value obtain in step 4 with equivalent character and apply the Rail Fence Method to transpose the position by 1. Write the ASCII value of character.

Step 6. Convert into binary format and apply logical NOT.

Step 7. Replace with decimal values obtain in step 6 and also replace with ASCII equal character.

Step 8. Final got cipher text.

The steps followed in the proposed decryption algorithm are as follows:

Step 1. The cipher text i.e. ASCII equivalent character is then replaced by its decimal equivalent value.

Step 2. Convert the binary equivalent of the decimal number calculated in Step 1 and Apply the Logical NOT to the binary value.

Step 3. Calculate its decimal equivalent to write the character value based on ASCII value.

Step 4. Apply the reverse rail fence method to transpose the position by 1.Write the numeric code for that character.

Step 4: Now add 26 to that numeric code. (Alphabet Number + 26)

Step 5: Then subtract the key from the result obtained from step 4.

Step 6: Final got plain text.

The proposed algorithm is shown with the help of flow chart in Figure 5.

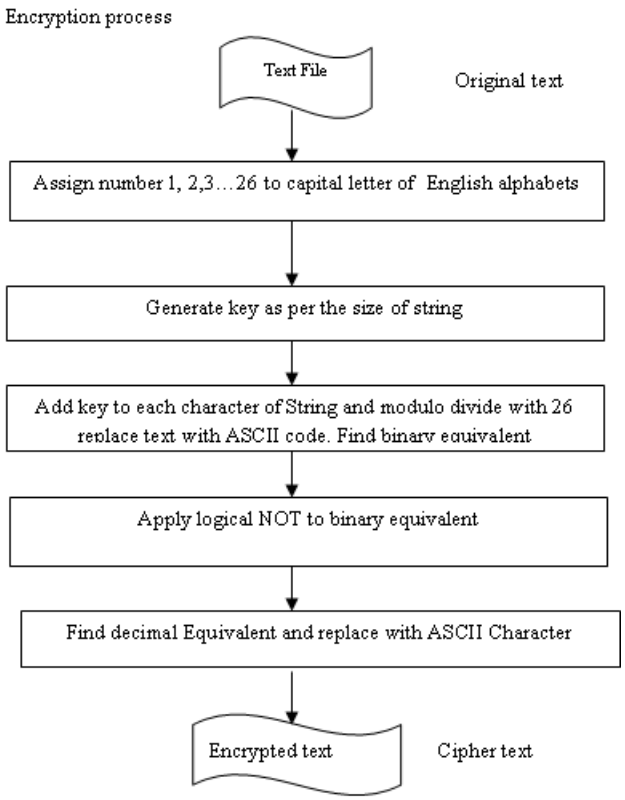

Figure 5 Architecture of Proposed Approach

VII. EXPERIMENTAL ANALYSIS

The performance of proposed algorithm is evaluated and compares it with symmetric key cryptography. The experiments were performed on i3 processor (2.5GHz Intel Processor with 4M cache memory), 2GB main memory and 400 GB secondary memory and running on Windows 7. The algorithms are implemented in using C# Dot net frame work version 10. The simple text file is used for encryption and decryption method. . The text file is created using note pad to perform the encryption process. The implementation chooses text file from a selected location. User create text file anywhere in computer memory. When encryption process is completed a file with encrypted text is generated and saved at a location given by the user. For the decryption process user

select an encrypted file from the location file and repeat the same process. The parameters used for comparison are execution time and memory required for encryption and decryption. Figure 6 shows the implementation of symmetric approach and Figure 7 shows the implementation of the proposed algorithm.

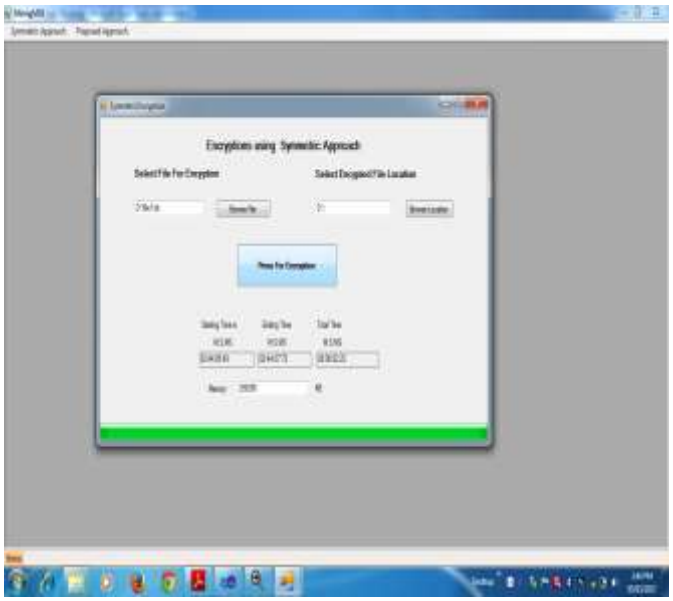

Figure 6 Encryption using Symmetric Approach

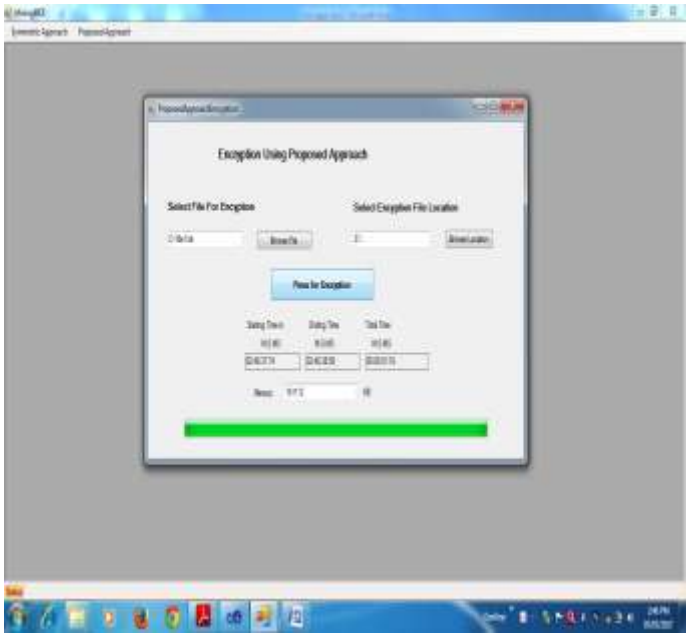

Figure 7 Encryption using Proposed Approach

VIII. COMPARISON WITH GRAPH

From the experimental analysis it has been observed that proposed approach takes less time for encrypting given text as compared to the symmetric approach. The proposed approach compares the result on the basis of file size and execution time for encryption. Table 1 shows comparison between symmetric approach and proposed method on the basis of file size and execution time for encryption. Figure 8 shows the comparative graph for the execution time of the symmetric approach and proposed approach of different file size.

Table 1 Execution Time for Symmetric & Proposed Approach

File Size in KB	Symmetric Approach	Proposed Approach
10	1067	1032
20	2056	1272
50	3212	2142

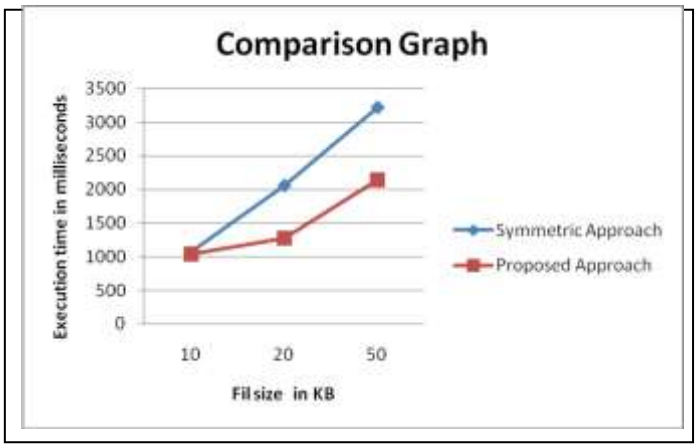

Figure 8 File Size and Execution Time for Encryption

IX. CONCLUSION

The main objective of the proposed approach is to minimize execution time for encryption and decryption. The proposed approach reduces execution time for encryption and decryption and improves the performance when compared to the symmetric approach. The proposed algorithm is now extended to minimize the number of keys required for encryption and decryption in future research work.

REFERENCES

[1] William, "Cryptography and Network Security Principles and Practice", Fifth Edition, Pearson Education, Prentice Hall, 2011.

[2] Schneier B., "Applied Cryptography", John Wiley& Sons Publication, New York, 1994.

[3] A. Kahate "Computer and Network Security" 2nd Edition, Tata Mc-Grew – hill Publisher ltd, 2011.

[4] Ayushi "A Symmetric Key Cryptographic Algorithm" International Journal of Computer Applications (IJCA) ISSN : 0975 – 8887) Vol. 1 – No. 15 , February 2010.

[5] V. Shokeen & N. Yadav "Encryption and Decryption Technique for Message Communication" International Journal of Electronics & Communication Technology ISSN : 2230-7109(Online) | ISSN : 2230-9543(Print) IJECT Vol. 2, Issue 2, June 2011.

[6] B. .R. Kumar & Dr. P. R. K. Murti "Data Encryption and Decryption process Using Bit Shifting and Stuffing (BSS) Methodology". International Journal on Computer Science and Engineering (IJCSE) ISSN: 0975-3397 Vol. 3 No. 7 July 2011.

[7] Ch. S Reddy, Ch. Sowjanya & P. Praveena " Poly-alphabetic Symmetric Key Algorithm Using Randomized Prime Numbers" International Journal of Scientific and Research Publications, Volume 2, Issue 9, September 2012 1 ISSN 2250-3153.

[8] M. Agrawal & P. Mishra "A Comparative Survey on Symmetric Key Encryption Techniques" International Journal on Computer Science and Engineering (IJCSE) ISSN: 0975-3397 Vol. 4 No. 05 May 2012.

[9] K. Pandey & V. Rangari "An Enhanced Symmetric Key Cryptography Algorithm to Improve Data Security International Journal of Computer Applications (0975 – 8887) Volume 74– No. 20, July 2013.

[10] O. Mohammad Awad Al-Hazaimeh "A New Approach for Complex Encrypting and Decrypting Data" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2, March 2013.

[11] R. Arora & A. Parashar "Secure User Data in Cloud Computing Using Encryption Algorithms" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926.

[12] V. Sukhraliya & S. Chaudhary "Encryption and Decryption Algorithm using ASCII values with substitution array Approach". International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013.

[13] Sruthi B. Asok, P. Karthigai kumar & Sandhya R "IRIS Based Cryptography" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 2, February 2013.

[14] M. Ebrahim & S. Khan "Symmetric Algorithm Survey: A Comparative Analysis International Journal of Computer Applications (0975 – 8887) Volume 61– No.20, January 2013.

[15] D. Nagde, R. Patel & D. Kelde "New Approach for Data Encryption using Two Way Crossover". International Journal of Computer Science and Information Technologies, Vol. 4 (1), 2013, 58 – 60.

[16] Ezeo for C. J., Ulasi A. G "Analysis of Network Data Encryption & Decryption Techniques in Communication Systems" International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 12, December 2014.

[17] S. R. Shinge & R.Patil "An Encryption Algorithm Based on ASCII Value of Data". (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7232-7234.

[18] Mitali, V. Kumar & A. Sharma "A Survey on Various Cryptography Techniques". International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Web Site: www.ijettcs.org Email: editor@ijettcs.org Volume 3, Issue 4, July-August 2014.

[19] S. Tayde & S. Siledar "File Encryption, Decryption Using AES Algorithm in Android Phone" International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) ISSN : 2277 128X Vol. 5 Issue 5 May 2015.

[20] Zaeniah, Bambang Eka Purnama "An Analysis of Encryption and encryption Application by using One Time Pad Algorithm" International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 6, No. 9, 2015