International Journal of Information Science and Computing 3(2): December, 2016: p. 99-108
DOI : 10.5958/2454-9533.2016.00012.0

Investigation of Efficient Cryptic Algorithm for Text using SM Crypter

Shivlal Mewada[1], Pradeep Sharma[2] and S.S. Gautam[3]

[1]Dept. of Computer Science, MGCGV, Chitrakoot, Satna M.P., India
[2]Dept. of Computer Science, Govt. Holkar Science College, Indore M.P., India
[3]Dept. of Computer Science, MGCGV, Chitrakoot, Satna M.P., India

Corresponding author: shiv.mewada@gmail.com

Abstract

Without information security, number of problem arises with the security of different text datafiles (.doc, .txt, .pdf, .ppt, .xls) etc.important data andsecurity is required to send with assurance of confidentially, integrity and authenticity of information over the network or web. So, there is a need to have a method to protect the information and avoid the unauthorized access of text data over insecure communication environment. Cryptography algorithms play a vital role in providing the information security against malicious attacks.Cryptography methods are based on symmetric and asymmetric encryption algorithms. It is challenging researchers to find out efficient encryption algorithm and to implement cryptic algorithm. There are many organizations working on SKC cryptic algorithms for safe data communication web. Symmetric encryption is widely used technique. In this paper, we present Encipherment and Decipherment of Symmetric Key Cryptography Algorithm for Text using SMCrypter with some block cipher SKC algorithms.

Keywords: SMCrypter, Symmetric Key Cryptography Algorithms, Cryptosystem, Text, Encipherment, Decipherment

Without information security, number of problem arises with the security of different text datafiles (.doc, .txt, .pdf, .ppt, .xls) etc.important data andso security is required to send with assurance of confidentially, integrity and authenticity of information over the network or web. So, there is a need to have a method to protect the information and avoid the unauthorized access of text data over insecure communication environment.

There are several techniques to keep the information confidential from hackers and malicious attacks. Some are biometrics, passwords and cryptography. Traditional passwords aren't so good for this job due to their low entropy. Biometrics methods produce harmful effects on the human body (beings) and it is more costly. For these above discussed problems cryptography is the best solution for information

security on network or web. The main goal of cryptography is keeping data secure form and important files from unauthorized attackers.

Cryptography [1] method has a long history to store sensitive data or transmit it across insecure web (i.e. the Internet) so that it cannot be read by anyone except the intended recipient, where the crypto method is a set of several algorithms combined with keys to convert the plain-textto cipher-text (hidden data) and convert it back in the intended recipient side to the original message. Information cryptography mainly is the scrambling of the content of information, such as text, image,audio, video and so forth to make the data unreadable, invisible or unintelligible during transmission or storage called Encryption. There are two general categories for key based Encryption algorithm first one is calledSymmetric algorithm which uses a single key to encrypt the plain text and decrypt the Cipher text. Second is Asymmetric algorithm which uses two different keys a public key [2] to encrypt the plain text, and a private key to decrypt the cipher text [3].

Exchange of textual documents is word, excel, ppt. and business report needs encryption for secure exchange. For this encryption or decryption with various key files are done with longer key with large no of algorithms. Like; AES, 3DES, Blowfish, Twofish, RC6 and more.

The major issue to design any encryption and decryption algorithm is to improve the security level. Therefore, this paper investigation of performance analysis for exchange of textural documents is word, excel ppt. and business is presented. This paper aims to propose anefficient symmetric algorithm to improve the security level and increase the performance by minimizing a significant amount of delay time (encryption and decryption time) to maintain the security and makes comparative study [4].

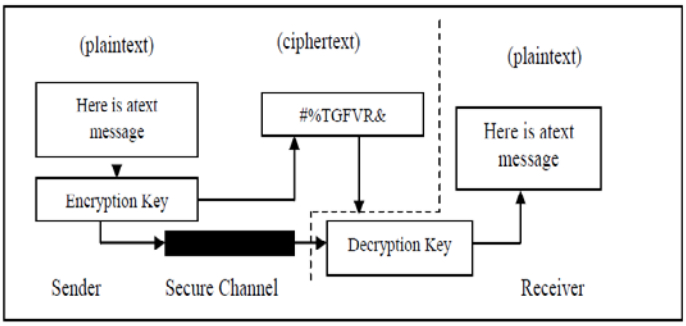

Fig. 1: Basic Cryptographic Model

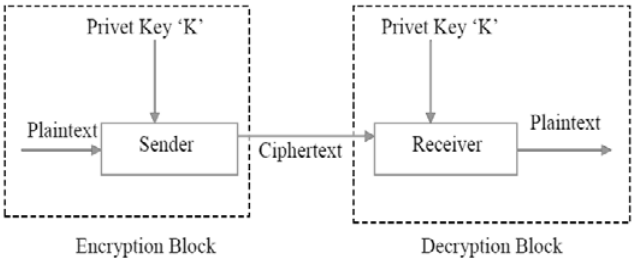

Fig. 2: Encryption and Decryption using Single/Private Key

In Fig. 2, Private Key 'K' is used for Encryption and Plaintext is converted into Ciphertext. Same Private Key 'K' is used for Decryption and Ciphertext is again converted back into Plaintext.

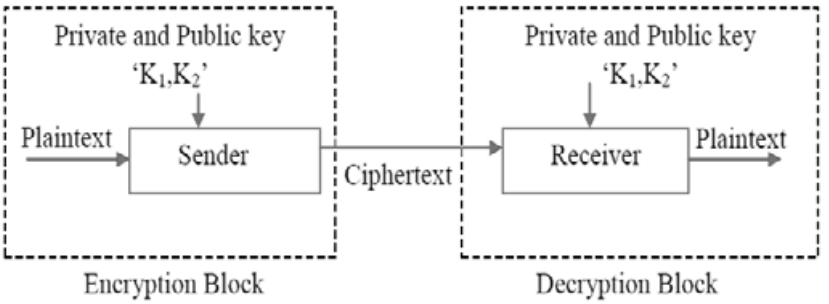

Fig. 3: Encryption and Decryption using Private and Private Key

In Fig .3 'K1, K2'are Public Key for Encoding of Plaintext to converted into Cipher text.At receiving end Same Key 'K1, K2' is used for recover plaintext from Cipher text. K1 is publically distributed and K2 is used as a secret key.

Background and Related Work

This section involves the work done by the several research scholars in the field of symmetric cryptographic algorithm for information security. From the literature survey (books, magazines, journals and others), observation have been drawn andstated at the end of this section. Finally from the observation objectives of this work havealso been derived.

For encryption and decryption of same type of files numerous symmetric algorithms are available in the literature , for finding out better method to optimize communication cost[5] presents results of comparison for AES algorithm.Apart from efficient algorithm search, the classification of these methods for behavior analysis has been presented in [6, 7].

The generation of symmetric key is a challenge, In [8] key generation has been presented using Cassini formula. In[9] key generation has been presented by using location information of sender and receiver. In [10] and [11] the implementation of these approaches has been presented. The analysis of key generation methods has been discussed in [12] for analysis of cipher text. The application of data mining in analysis of cipher text for useful information such as keysize has been presented in [13].Association rule generation has also been presented in [14].Thus auditing of cryptic algorithm is essential step for development of secure information exchange system.

In [15, 16*]* compared the advance encryption standard algorithm with several modes of operation (block cipher) and RC4 algorithm (stream cipher) in terms of memory utilization, CPU time, encryption time, decryption time, and throughput at various settings like variable key size and variable data packet size. In [17] presented an efficient block cipher encryption methods based on cubical techniques and improved key. In [18] proposed a method to protect the data in faster way by using classical cryptography.

In [19] proposed a new block cipher SKC algorithm named TACIT encryption method for secure routing. In[20] proposed an image encryption using advanced hill cipher algorithm or encrypt an image. In [21] worked on secret data communication system using steganography, AES and RSA. In [22] proposed an efficient symmetric key cryptography algorithm for information security.

Architecture of SKC algorithms

Advanced Encryption Standard (Rijndael) [5,6,7, 23]: With block sizes 128, 192 and 256 bits., key size - 128,192 and 256 bits. It depends on the length of key e.g. 10 round for 128 bit key, 12 rounds for 192-bit key and 14 rounds for 256 bit keys. In Rijndael algorithm, plain text transformed into cipher text after passing through the different stages such as byte substitution, row shift, column and round key.

Triple Data Encryption Standard: 3DES performs 3 iterations of DES with 3-different keys. For 64 bit plain text with 16x3 rounds + length of Key 168-bits+ permutation into 16 sub- keys(48- bit length) + 8 substitution boxes in reverse order for decryption [5,6,7, 24].

Blowfish Algorithm: It includes key-expansion and data-transformation part with 64 bit input text + 16 iteration, key length up to 448 bits, 18 sub- keys each of 32- bit length can be used on 32 or 64-bit processors[5,6,7,25].

RC6: With block size of 128-bit input/output blocks (32-bit words) and key sizes of 128, 192, and 256 bits. RC6 is a parameterized algorithm where the block size, the key size, and the number of rounds are variable [5,6,7,26]. It may be parameterized to support a wide variety of word-lengths, key sizes, and number of rounds. RC6 is very similar to RC5 in structure, using data-dependent rotations, modular addition, and XOR operations; in fact, RC6 could be viewed as interweaving two parallel RC5 encryption processes, although RC6 does use an extra multiplication operation not present in RC5 in order to make the rotation dependent on every bit in a word, and not just the least significant few bits.

Twofish: With a block size of 128 bits and key size ranging from 128 to 256 bits, and is optimized for 32-bit CPUs. It was one of the 5 finalists of the AES contest, but it was not considered for standardization. Twofish is correlated to the previous block cipher Blowfish [5,6,7].

Table: 3.1: Skc Algorithms Architecture [5,6,7,]

Algorithm	Algorithm Structure	Block sizes (Plain/ Cipher)	Key Size (Max/ Min)	Cipher Type	Number of Rounds
AES	S-permutation network	128 bits	128,192,256	Block cipher	10,12,14
3DES	Feistel cipher network	64 bits	168	Block cipher	48
Blowfish	Feistel cipher network	64 bits	128-448	Block cipher	16
Twofish	Feistel cipher network	128 bits	128, 192, 256	Block cipher	16
RC6	Feistel cipher network	128, 256	128, 192, 256	Block cipher	20 (recommended)

Methodology

We choosing more efficient symmetric key cryptographic encryption and decryption techniquehave been an issue. To choose the best SKC algorithm from a list of symmetric key encryption and decryption algorithms like: AES, Blowfish, 3DES, RC6 and Twofish, we can encryption and decryption them first to get the best out of them. But for that we need some tool to encryption and decryption their working. Also there should be some parameters like key size, data size, encryption and decryption time for judging which one is the best among them.

Proposed Methods

We may analyze SKC encryption and decryption algorithms using the web application of SMCrypter, which provides actual statistics generated during encryption or decryption in several cases. It supports 4 cases of encryption and decryption and provides manytypes of graphs.

Following two categories of graphs supported by SMCrypter are used as follow:

Category I: Data size v/s execution time for encryption using a text data files.

Category II : Data size v/s execution time for decryption using a text data files

Experimental Design

For our experiment, We Designed SMCrypter and use a SMCrypter. SMCrypter has been created by us using various programming technologies such as JavaScript (JAVA), HTML, PHP, CSS, JpGraph, and Bootstrap.

In this work, we are trying to find out performance *analysis* of five symmetric key cryptographic algorithms like:AES, 3DES, Blowfish, Twofish and RC6 on different text file size range from 10KB to 1042KB. Based on the performance analysis and result, we will conclude that which algorithm is better to use based on different performance parameters.

We have considered the following parameters for performance analysis of SKC encryption algorithms on certain criteria:Key size, Data size, Encryption time, Decryption time etc.

Initial offline Simulation setup: The simulation has been done on a machine with the specifications:Processor-Intel i5-3230M (3rd generation) with 2.6GHz clock speed, RAM-4 GB, HDD-500 GB, Graphics-4GB. With these specifications the performances are gathered. In this paper the simulation have taken place for text files from the size 10 kb – 2618 kb.

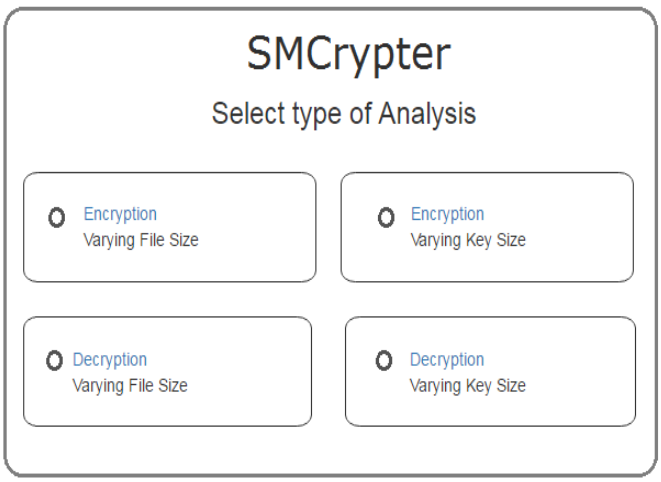

Fig. 4: Home Screen of SMCrypter

Performance Analysis, Result and Discussion

In order to analyze the performance of conventional SKC algorithms various combinations of data of different size and keys of different size are required. The SMCrypter tool has taken a set of data files(doc, .txt, .pdf, .ppt, .xls) and key with different sizes for this performance analysis. Some of our analytical results match with the results obtained by other researchers [27]. The different results achieved in the form of different graphs and tables for various symmetric key cryptography algorithms are given below.

Fig. 4: Interface of Select data file for graphs

Performance analysis for encryption of various SKC cryptic Algorithms

The Comparative performance of AES, 3DES, Blowfish,TwoFish and RC-6 algorithm over various text files with variable encryption key size and corresponding time taken to generate encrypted text files is discussed in this section in great details. The counter part of this process that is decryption of encrypted text files (processed with various key lengths) is assumed equivalent to encryption time. Here simulation results corresponding to four Input Text files (1,2,3,4 KB respectively and corresponding approximate binary representations are 0.6865234375,1.3525390625, 2.5595703125,3.1630859375 KB) of different length has been fed to simulator to a specific-Cryptic module and corresponding encryption time in seconds is expressed in second column. Please refer Table 3.12 and Table 3.13 Text file size v/s. execution time analysis for encryption using a key with 4 different size text files. Corresponding bar-chart represents performance of RC6 algorithm in Fig. 3.21 and 3.22.

Table 2: Encryption Time in Second with input key of India Key

File Size (Text)	AES Algorithm	**BlowFish**	3DES	**TwoFish**	RC6
0.6865234375 kb	0.000022	0.000024	0.000054	0.000217	0.001479
1.3525390625 kb	0.000021	0.000025	0.000079	0.000351	0.007884
2.5595703125 kb	0.00003	0.000038	0.000134	0.000662	0.015021
3.1630859375 kb	0.000035	0.000046	0.000168	0.000824	0.018437

Table 3: Encryption Time with input key of ndia

File Size (Text)	AES Algorithm	**BlowFish**	3DES	**TwoFish**	RC6
0.6865234375 kb	0.000023	0.000023	0.000049	0.000223	0.004132
1.3525390625 kb	0.000028	0.000025	0.000077	0.000363	0.007922
2.5595703125 kb	0.000038	0.000039	0.00014	0.000664	0.015009
3.1630859375 kb	0.000045	0.00005	0.000174	0.000829	0.01851

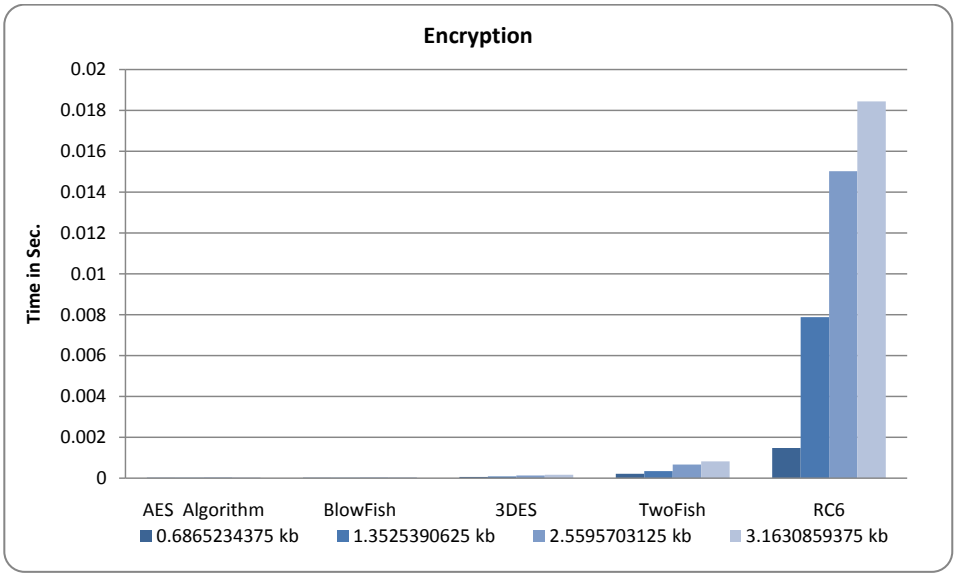

Fig. 5: File size v/s Encryption time for Image file of different sizesusing input key of ´India"

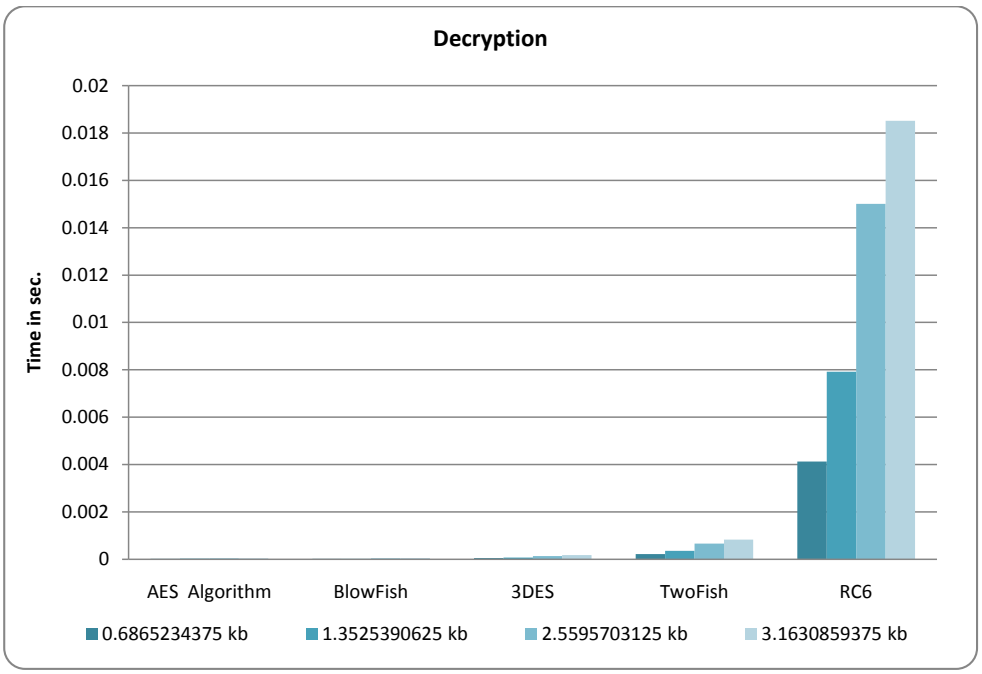

Fig. 6: File size v/s Decryption time for Image file of different sizes using input key of ´India"

From above discussion it can be deduced that efficient algorithm for security on network or web AES play a vital role in providing the TEXT information security against their competitive algorithms. With the comparative investigation with variable key size and file size we have observed that AES variants

are efficient encryption algorithm and to implement cryptic algorithm. For text information security the use of correct encryption method. Symmetric encryption is widely used technique In future the analysis can be extended for variants of text files such as word, excel ppt. can be investigated.

Conclusion and Future work

Different SKC algorithm have been analyzed for performance evaluation for several matrixes like different data type, data size, key size, encryption time and decryption time and tested how the encryption time varies for different SKC algorithms. This paper presents various state of art symmetric cryptography algorithm for encryption of text files.Here all these algorithms have been analyzed for text file encryption and decryption performance. The Experiments investigation demonstrates AES shows better performance, over its competitors in terms of encryption time, decryption time, CPU process time. The performances over huge range of text files like are yet to be investigated. After analysis of all parameters, AES was found to be most suitable encryption algorithm in four modes. In future, this would be beneficial for document and article management system including news. The future work can be compromise of implementing this work for cloud computing environment and the efficiency of the cryptic system can be improved even more by implementing it in Hadoop environment.

References

1. J.-S. Coron, “What is cryptography”, IEEE Security & Privacy, Vol. 4, Issue: 1, pp(70-73) Feb. 2006. DOI: 10.1109/MSP.2006.29
2. R.Rivest, A. Shamir, L.Adleman, “A method for obtaining digital signatures and public-key cryptosystems” Communications of the ACM, Volume 21 Issue 2, pp(120-126), Feb. 1978. Doi:10.1145/359340.359342
3. William Stallings, “Cryptography and network security: principles and practices”, Pearson Education India, 7th edition 2009.
4. H. Mohan, and R. Raji. “Performance Analysis of AES and MARS Encryption Algorithms”. International Journal of Computer Science Issues (IJCSI), Vol. 8, issue 4. July 2011.
5. Shivlal Mewada, Pradeep Sharma, S. S. Gautam, “Exploration of efficient symmetric AES algorithm”, IEEE Symposium on Colossal Data Analysis and Networking (CDAN), pp (1-5), Mar 2016. DOI: 10.1109/CDAN.2016.7570921
6. Shivlal Mewada, Pradeep Sharma, S. S. Gautam, “Classification of Efficient Symmetric Key Cryptography Algorithms”, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 14, No. 2, pp(105-110.), Feb 2016
7. Shivlal Mewada, Pradeep Sharma, S. S. Gautam, “Exploration of Efficient Symmetric Algorithms”, IEEE-International Conference on Computing for Sustainable Global Development, pp() March, 2016
8. Prajapat, Shaligram, Amber Jain, and Ramjeevan Singh Thakur. “A novel approach for information security with automatic variable key using Fibonacci Q-matrix.” IJCCT 3.3 (2012): 54-57.
9. ShaligramPrajapat, Ramjeevan Singh Thakur, “Key Diffusion Approach for AVK based Cryptosystem”,In Proceedings of the Second International Conference on Information and

Communication Technology for Competitive Strategies ICTCS-16 published by ACM, Article No. 78, 2016. doi : 2905055.2905288

10. Shaligramprajapat, R. S. Thakur," Realization of information exchange with Fibo-Q based Symmetric Cryptosystem" ,International Journal of Computer Science and Information Security, IJCSIS, Vol. 14(2), pp. 216-223, 2016.

11. Prajapat, Shaligram, Ramjeevan Singh Thakur. "Markov Analysis of AVK Approach of Symmetric Key Based Cryptosystem."In proceedings of Computational Science and Its Applications--ICCSA 2015.Springer International Publishing. pp. 164-176. , 2015.

12. Prajapat, Shaligram, Ramjeevan Singh Thakur."Cryptic Mining: Apriori Analysis of Parameterized Automatic Variable Key based Symmetric Cryptosystem." International Journal of Computer Science and Information Security, Vol. 14 (2), pp. 233- 246, 2016.

13. Prajapat, Shaligram, Ramjeevan Singh Thakur. "Optimal Key Size of the AVK for Symmetric Key Encryption." In Covenant Journal of Information & Communication Technology,Vol.3(2), pp. 71-81. (2015)

14. ShaligramPrajapat, Ramjeevan Singh Thakur, "Cryptic Mining for Automatic Variable Key Based Cryptosystem", Elsevier Procedia Computer Science ,Vol.78, pp. 199-209, 2016.

15. NidhiSinghal, J.P.S.Raina, Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology, Vol. 1, Issue-3, pp(117-181), July 2011.

16. Neha Joshi, Megha Singh, Surabhi Shah, "A New Encryption Algorithm to Increase Performance & Security through Block Cipher Technique", Int. J. of Engg. Science and managment, Vol. 5, Issue 4, pp(73-78), Dec 2015 .

17. S KTripathi1, U K Lilhore, "An Efficient Block Cipher Encryption Technique Based on Cubical Method and Improved Key"Imperial Journal of Interdisciplinary Research", Vol-2, Issue-6, pp (373-377), June 2016.

18. Raghu M E and Ravi shankar K C, "Application of Classical Encryption Techniques for Securing Data- A Threaded Approach", International Journal on Cybernetics & Informatics (IJCI) Vol. 4, No. 2, pp(125-132), April 2015.

19. P. Gope, A. Singh, A Sharma and N. Pahwa, "An Efficient Cryptographic Approach or Secure Policy Based Routing", IEEE Journal on Selected Areas in Communications, Vol. 1, pp. 359-363, 2013.

20. L. Buttyan, L. Czap and I. Vajda, "Detection and Recovery from Pollution Attacks in Coding Based Distributed Storage Schemes", IEEE Transaction on Dependable and Secure Computing, Vol. 8, No. 6, pp. 824-838, 2011.

21. S. F. Mare, M. Vladutiu and L. Prodan, "Secret data communication system using Steganography, AES and RSA", IEEE: International Symposium for Design and Technology in Electronic Packaging, Vol. 2, pp. 339-344, Oct. 2011.

22. S. Verma, R. Choubey and R. Soni, "An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security", International Journal of Emerging Technology and Advanced Engineering, Vol. 1, pp(18-21), July 2012.

23. James Neuchâtel at. al., "Report on the Development of the Advanced Encryption Standard (AES)", Journal of Research of the National Institute of Standards and Technology, Volume 106, Number 3, May–June, pp(511–577) 2001.

24. S. Sony, H. Agrawal, M. Sharma, "Analysis and comparison between AES and DES Cryptographic Algorithm", International Journal of Engineering and Innovative Technology, Vol. 2, Issue 6, pp(362-365), December 2012.

25. Alabaichi, A., Ahmad, F., Mahmod, R., "Security analysis of blowfish algorithm", IEEE: 2nd International Conference on Informatics and Applications (ICIA-13), 23-25 Sept. 2013, pp(12 - 18), DOI: 10.1109/ICoIA.2013.6650222, Print ISBN:978-1-4673-5255-0

26. Elminaam, D. S. A., Kader, H. M. A., &Hadhoud, M. M. (2008). Performance Evaluation of Symmetric Encryption Algorithms. IJCSNS International Journal of Computer Science and Network Security, 8(12), 280-286.

27. Elminaam D.S., Abdual H.M., Hadhoud M.M., "Evaluating The Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vol-10, No-3, pp. 216-22, 2010.