International Journal of Future Generation Communication and Networking
Vol. 13, No. 1, (2020), pp. 99-107

Comparative Investigation of SKC Algorithms for Secure Information with different Parameters

Shivlal Mewada[1], S.S. Gautam[2] and Pradeep Sharma[3]
[1,2]Dept. of Computer Science (Physical Sciences), MGCGV, Chitrakoot, India
[3]Dept. of Computer Science, Govt. Holkar Science College, Indore, India
e-mail: shiv.mewada@gmail.com

Abstract- *Today's era communication and transmission security of static and dynamic data is essential, and information security is also a primary concern for every secure communication system. It is necessary to secure confidential static and dynamic data from unknown users. Cryptography methodologies have a vital role in providing security to these confidential static and dynamic data from unauthorized attacks. In this paper, we investigate a more secure and efficient cryptic algorithm, provide the performance of SKC algorithms and also comparison analysis of some SKC family cryptic ciphers algorithms on the basis of computing encryption time and decryption in second with the variation of different file- data types, data size, key sizes, etc.*

Keywords- *Data Size, Data Types, Decryption Time (D_T), Encryption Time (E_T), Key Sizes, SKC Algorithm*

I. INTRODUCTION

In recent years online apps are exploring day by day such as social site, online banking, online games, online purchasing, stock market, share market and online bill payments and more. Without security these apps are impossible, cryptography methods provides the security to the data which is share and exchange over internet (online). The cryptography methods are usually classified into two types: Symmetric key encryption (SKC) and Asymmetric key encryption (AKC). In SKC, only one key is used to encipherment and decipherment data. The key is distributed before transmission between entities. Therefore, key plays an important role in SKC encryption. Strength of SKC depends on the key size used. For the same algorithm, encryption using longer key is harder to break than the one done using shorter key. The representative SKC algorithms include Blowfish, AES, RC2, DES, 3DES, and RC5. AKC is used to solve the problem of key distribution. In AKC encryption, both keys are used -private key and public key. Public key is used for encryption and private key is used for decryption. All the Cryptographic algorithms are extensively used for security and privacy of internet networks.

The main objective of this paper, we investigate a more secure and efficient cryptic algorithm, provide the performance of SKC algorithms and also comparison analysis of some SKC family cryptic ciphers algorithms on the basis of computing encryption time and decryption in second with the variation of different file- data types, data size, key sizes, etc.

Rest of the paper is organized as follows, Section I contains the introduction of SKC Algorithms for Secure Information with different Parameters and main objective of this paper, Section II contain the related work of SKC Algorithms for Secure Information with different Parameters, Section III contain the methodology experimental set up and proposed SKC cryptic tool, Section IV describes results and discussion of this study, Section Vconcludes research work with future directions.

II. RELATED WORK

This section discusses some of the results obtained from other research papers to give more prospective about the performance of the SKC algorithms.

In recent years, many researchers and research organization has focused on the mechanization of SKC algorithms and the application of cryptic methods based on Encipherment and decipherment computing time.

Traditional Input-Cryptic algorithms get the pixels of the input file to transform into cryptic input file in variety of ways. The comparative performance analysis of these schemes is essential to explore the faster encipherment time such that encrypted input file is exchanged faster to the person. Perfection in the transformation back into input after decrypting it [1,2].

There is no doubt the way cloud computing has drastically changed the everyone's perception about cloud infrastructure which includes SaaS, IaaS, PaaS, XaaS and the Cloud computing has been considered as great innovation [3].

Cryptography is first step towards the security of the sensitive information of data owners in cloud storage. Various Cryptographic algorithms has been introduced from time to time to encrypt the data and mainly it has been seen that AES, 3DES, RC6, Twofish and Blowfish has been used for security purpose[4,5,6,7,8,9,10].

In [11], the selected SKC algorithms are AES, 3DES, Blowfish, and DES. By using these SKC algorithms the performance of encipherment and decipherment process of input files is considered and the throughput analysis is completed.

In [12] considered the performance of encryption algorithm for text files and it uses SKC algorithms of AES, DES and RSA algorithm. It is found that; first the E_T is computed. The time is taken to convert readable text to unreadable text is known as E_T. Comparing these SKC algorithms, RSA takes more time for computing process.
It [13] discussed the performance evaluation of SKC algorithms of AES and Blowfish.

III. METHODOLOGY

Methodology-Several the existing SKC symmetric key algorithms, choosing much efficient SKC cryptographic encryption and decryption method have been an issue. Proposed SKCrypter tool supports the user to choose a symmetric key based cryptic algorithm from a list of conventional cryptic algorithm, to performance analyse and compare these SKC algorithms to choose best out of them based on encryption time and decryption computing in second with the variation of different file- data types, data size, key sizes, which provides real statistics generated during encipherment and decipherment computing time in second with the following several cases.

Experimental Setup (offline setup)- The simulation results have been taken on the desktop Acer machine with the following specifications-Processor-Intel i5-3230M (5th Gen.) with 2.6GHz clock speed, RAM-6 GB (DDR-4), HDD-1TB, Graphicscard-4GB.

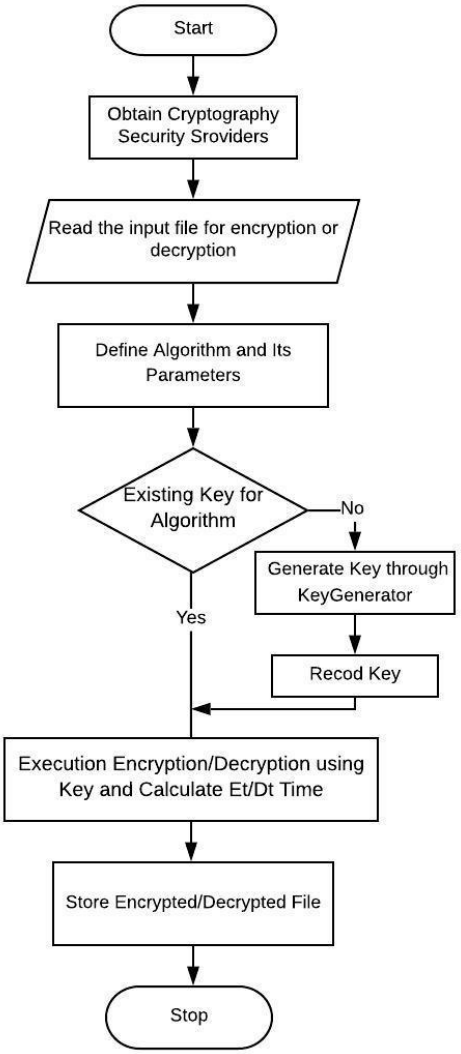

Figure 6: Execution Procedure of the Program Flow Control

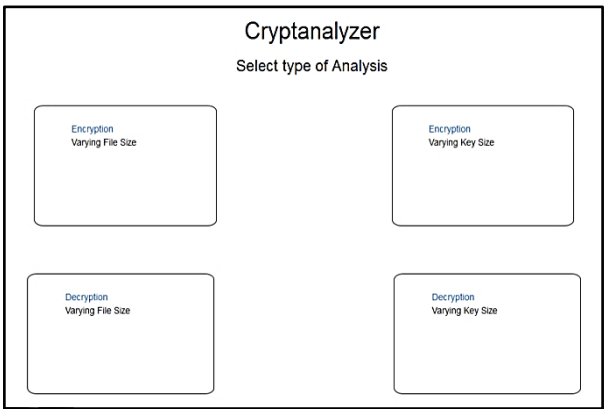

Figure 1: Home Screen of SKCrypter Took

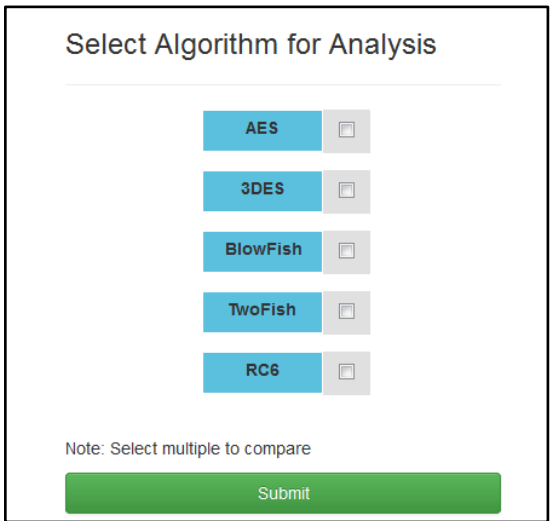

Figure 2: Interface of SKCrypter
(Varying File Size Encryption)

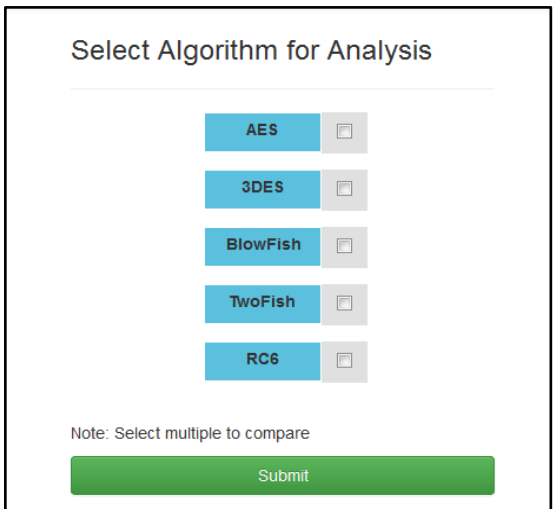

Figure 3: Category interface of SKCrypter
(Varying File Size Decryption)

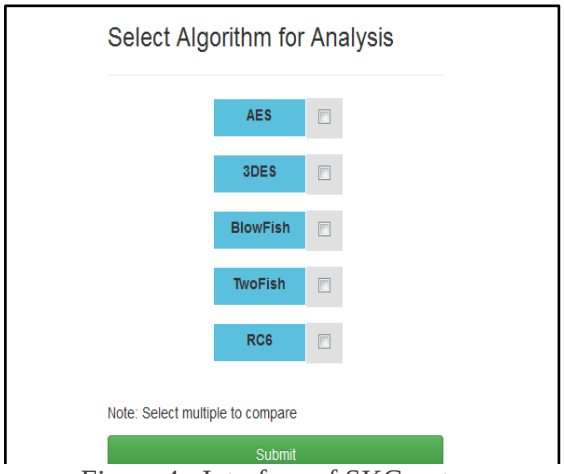

Figure 4: Interface of SKCrypter
(Varying Key Size Encryption)

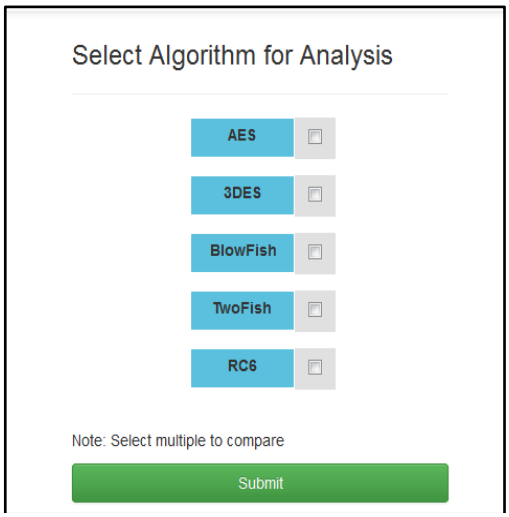

Figure 5: Interface of SKCrypter (Varying Key Size Decryption)

Cases A: Encryption of Static data or Dynamic data of different sizes with fixed key.
For first case, input files supplied to above tool varies with size of static data or dynamic data with fixed key size and encryption time has been recorded. The result (time) received has been presented in table form in the result section.

Cases B: Decryption of Static data or Dynamic data of different sizes with fixed key.
In second case focus is given on decryption time. For second case with the same input data supplied in case-A to above tool varies with size of input files with fixed key sizeanddecryption has been recorded. The result (time) received has been presented in table form in the result section.

Cases C: Encryption of Static data or Dynamic data of fixed size with Variable key sizes.
For third case with the same input file supplied in case-A to above tool varies with size of keyfilesandencryption time has been recorded. The result (time) received has been presented in table form in the result section.

Cases D: Decryption of Static data or Dynamic data of fixed size with Variable key sizes.
For fourth case with the same the same input file supplied in case-A to above tool varies with size of key files and decryption has been recorded. The result (time) received has been presented in table form in the result section.

IV. RESULT AND DISCUSSION

This section gives detailed description about the experimental results which is used to evaluate the performance of encryption algorithms. In order to analyse the performance and comparative analysis of SKCryptic algorithms have been tested with various combinations of static and dynamic information of different sizes and keys of different sizes is required.

The SKCryptic tool has taken a set of static data or dynamic data and key with different sizes for this performance analysis. The several results achieved in the form of different tables and graphs for various SKC algorithms are given below.

Experimental results corresponding to encipherment and decipherment of four input files of sizes 18KB, 20KB, 220KB, and 240KB respectively with fixed key size are presented in table-1 and table-2. Corresponding column chart representation of performance of SKC algorithmsare presented in fig.1 and fig.2.Table-3 and table-4shows the experimental results corresponding to encipherment and decipherment of fixed inputfiles of 18KB with variable key sizes of 0.007KB, 0.008KB, 0.009KB, and 0.0010KB respectively.

Corresponding column chart representation of performance of SKC (3DES, Blowfish, and AES)algorithms are depicted in fig.3 and fig.4.

The Comparative performance analysis of SKC(3DES, Blowfish, and AES) algorithms over Inputfiles of fixed size and different sizes along with variable fixed encipherment and decipherment keys and variable encipherment/decipherment keys have been examined and corresponding encipherment/decipherment time taken to generate encrypted/decrypted input files is presented in this section in great details.

Table-1 and table-2displaysencipherment and decipherment time taken by SKC algorithms discussed above with variable inputfiles and fixed key and table-3 and table-4displaysencipherment/decipherment time taken by SKC algorithms discussed above with fixed inputfilesfile and variable key sizes.

Here experimental results corresponding to four input files 18KB, 20KB, 220KB, and 240KB respectively with fixed key of 0.008KB is represented by fig 1 and fig 2 respectively.

Table-3 and table-4displaysencipherment and decipherment time taken by SKC algorithms discussed above with fixed inputfiles of size 18KBand Key sizes of 0.007KB, 0.008KB, 0.009kb and 0.0010KB respectively. Intable-3 and table-4displays encipherment and decipherment time taken by SKC algorithms discussed above with fixed inputfilesfile and variable key sizes.

Here experimental results corresponding to four Key sizes of 0.007KB, 0.008KB, 0.009KB, and 0.0010KB with fixed input files of size 18BKis represented by fig.3 and fig.4 respectively.

Table 1: Encryption Time (E_T) Taken by SKC algorithms with fixed key of file size .007Kb

File Size	AES	Blowfish	3DES
18KB	0.000317	0.00446	0.001977
20KB	0.000425	0.00624	0.002721
220KB	0.004655	0.006728	0.030205
240KB	0.005029	0.007256	0.032761

Table 2: Decryption Time (D_T) Taken by SKC algorithms with fixed key of file size .007Kb

File Size	AES	Blowfish	3DES
18KB	0.000308	0.000422	0.002006
20KB	0.000445	0.000588	0.002600
220KB	0.004609	0.006422	0.030402
240KB	0.005112	0.006956	0.033042

Table 3: Encryption Time (E_T) Taken by SKC algorithms with fixed inputfiles of 18KB with variable key Files

Key Size	AES	Blowfish	3DES
0.007KB	0.000320	0.000462	0.002010
0.008KB	0.000318	0.000471	0.001946
0.009KB	0.000317	0.000457	0.002003
0.0010KB	0.000330	0.000458	0.002013

Table 4: Decryption Time (D_T) Taken by SKC algorithms with fixed input files of 18KB with variable key files

Key Size	AES	Blowfish	3DES
0.007KB	0.000312	0.000429	0.001980
0.008KB	0.000313	0.000430	0.001982
0.009KB	0.000317	0.000431	0.001985
0.0010KB	0.000323	0.000435	0.001987

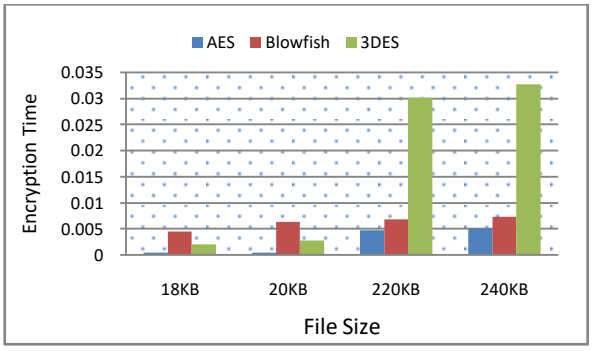

Figure.1: Encryption Time (E_T) of variable input files with fixed key

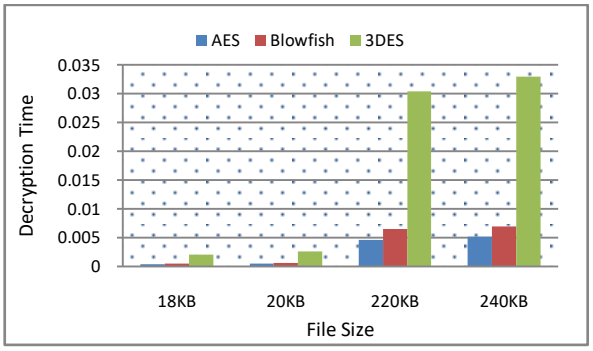

Figure.2: Encryption Time (E_T) of variable input files with fixed key

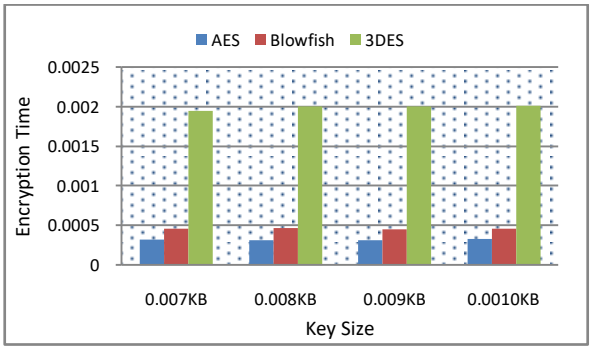

Figure.3: Encryption Time (E_T) of Fixed Input file with Variable key size

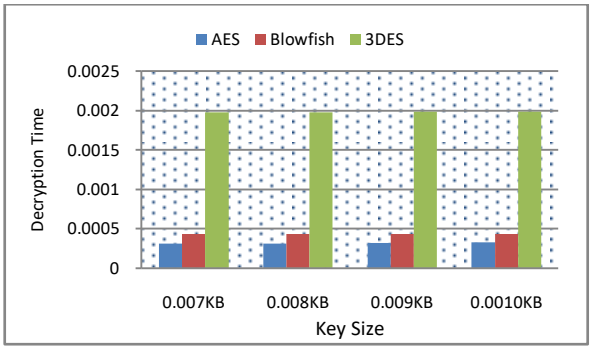

Figure.3: Decryption Time (D_T) of Fixed Input file with Variable key size

V. CONCLUSION

After analysis of experimental work, we have observed that in case of encryption time (E_T) taken by SKC algorithms for variable input files with fixed key of file size .007KB, SKC AES takes less time than SKC algorithms of Blowfish and 3DES.

In case of decryption time (D_T)taken by SKC algorithms for variable input files with fixed key of file size .007KB, Among AES, Blowfish and 3DESalgorithms, AES and Blowfish algorithm take a very less time in the comparison to 3DES algorithm and others SKC algorithms and encryption time (E_T) in 3DES is almost 8-9 times much compared to AES and Blowfish algorithm. We have found that with the increase in file size, encryption time also increases.

In case of encryption time (E_T)taken by SKC algorithms for fixed input file with variable key, AES and Blowfish algorithm take a very less time in comparison to 3DES algorithm and encryption time in 3DES algorithm is almost 8 times much compared to AES and Blowfish algorithms. Ithas been seen with fixed input file size and variable keys size encryption time is not varying too much and it is almost same with variable key file sizes. Therefore, impact of variable key on fixed file has little impact on encryption time.

In case of decryption time (D_T) taken by SKC algorithms for fixed input file with variable key, again AES and Blowfish algorithm takes almost a very less time than 3DES algorithm but decryption time (D_T) in 3DES is almost 7 times much compared to AES algorithm and also it has been seen that with fixed input file size and variable keys, decryption time is not varying too much and it is almost same with variable key file sizes. Therefore, impact of variable key on fixed file has little impact on decryption time.

The result shows that AES algorithm must be preferred over the encipherment and decipherment of input files in terms of encipherment time (E_T), and decipherment time (D_T) in security. However, when we look into the parameters like throughput and Memory utilization then Blowfish algorithm, must be preferred over AES algorithm.

REFERENCES

[1] Ashok Sharma, Ramjeevan Thakur, Shailesh Jaloree, "*Investigation of Efficient cryptic Algorithm for cloud storage*", Fourth International Conference on Recent Trends in Communication and Computer Networks, India, (2016) pp.23-30.

[2] Dimitrios Zissis, Dimitrios Lekkas, "*Addressing cloud computing security issues",* Future Generation Computer Systems, Vol. 28, (2012), pp.583–592.

[3] Vivek Raich, Pradeep Sharma, Shivlal Mewada, Makhan Kumbhkar, *"Performance Improvement of Software as a Service and Platform as a Service in Cloud Computing Solution*", International Journal of Scientific Research in Computer Science and Engineering, Vol.1, Issue.6, (2013), pp.13-16.

[4] Shivlal Mewada, Pradeep Sharma, S.S Gautam, *"Exploration of Efficient Symmetric AES Algorithm",* IEEE 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, (2016), pp.1-5.

[5] Shivlal Mewada, Sharma Pradeep, Gautam S.S., "*Exploration of Efficient Symmetric Algorithms"*, IEEE 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), Delhi, (2016), pp.663–666.

[6] Dorthy Elizabeth, Robling Denning, "*Cryptography and Data Security*", Addison-Wesley Publishing Company, Massachusetts, (1982), pp.301-340.

[7] D.W. Davies, W.L. Price, "*Security for Computer networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer*", Second Edition John Wiley & Sons, New York, (1989), pp.1-450.

[8] Noura Aleisa, "*A Comparison of the 3DES and AES Encryption Standards* ", International Journal of Security and Its Applications Vol.9, No.7, (2015), pp.241-246.

[9] Shivlal Mewada, Sharma Pradeep, SS. Gautam, "*Classification of Efficient Symmetric Key Cryptography Algorithms*", International Journal of Computer Science and Information Security (IJCSIS), Vol.14, No.2, (2016), pp.105-110.

[10] A. A. Yassin, A. A. Hussain, K. A. A. Mutlaq, *"Cloud authentication based on encryption of digital input using edge detection"*, AISP, India, (2015), pp.15-23.

[11] Gurjeevan Singh, Ashwani Kumar Singla, K.S.Sandha, "*Through Put Analysis of Various Encryption Algorithms*", IJCST Vol.2, Issue3, (2011).

[12] Shashi Mehrotra Seth, Rajan Mishra, "*Comparitive Analysis of Encryption Algorithms For Data Communication*", IJCST Vol.2, Issue 2, (2011)

[13] "*Performance Analysis of AES and BLOWFISH Algorithms* ", National Conference on Computer Communication & Informatics", School of computer science, RVS college of arts and science, March 07, (2012).