International Journal of Scientific Research in Computer Science and Engineering
Vol.4, Issue.6, pp.8-14, December (2016)

Research Paper

E-ISSN: 2320-7639

Investigation of Efficient Cryptic Algorithm for Storing Video Files in Cloud

A. Sharma[1*], R.S. Thakur[2], S. Jaloree[3]

[1]Department of Computer Science, Barkatullah University, Bhopal, India
[2]Department of Computer Application, MANIT, Bhopal, India
[3] Department of Mathematics, SATI, Vidisha, India

Corresponding Author: ashoksharmamca@gmil.com

Available online at: www.isroset.org

Received 30th Sep 2016, Revised 10th Oct 2016, Accepted 16th Nov 2016, Online 30th Dec 2016

Abstract— Cloud computing has brought good impact on the way, we use ICT resources. We are using various offerings of cloud computing which includes Flexible Computing Power,Flexible Storage capabilities, Platform as a service,Infrastructure as a service and software as a service on pay per use model. Nows a day the Customers are using their Smartphones to migrate their data in cloud storages but keeping in view of security issues in cloud storages, one must think of encrypting their data in cloud storages. Since in cloud storages, we keep various documents and we must think of fast encryption and decryption symmetric algorithm. but in literature, we do not find work that deals with investigation of efficient cryptic Algorithm for audio or video Files in cloud storages. In this paper, we are analyzing the performance of Cryptographic algorithms AES, Blowfish and DES algorithms in terms of encryption and decryption time taken depending upon the four factors namely file type, file size, key type and key size in case video files which may includes MPG, MPEG formats. For performance analysis, we have used Crypter tools deployed in Amazon Cloud and Tool is capable to encrypt and decrypt different types of files (in terms of size and format) depending upon variable or fixed type of key using AES, Blowfish and DES algorithms and the performance of these Cryptographic algorithms AES, Blowfish and DES algorithms can be analyzed in terms of time taken depending upon different types of files and different types of Keys. Analysis of the result obtained will help the user's to take decision regarding the selection of best symmetric algorithm to be used while uploading video data in cloud.

Keyword— *C*loud Computing, Cryptography, Encryption, Crypter Tool, Decryption

I. INTRODUCTION

The Cloud Providers have attracted various users to move their Video Files into free cloud storages or commercial sources because of various options in cloud storages and The Documents on Cloud or server repository is increasing rapidly. Therefore, it becomes necessary to ensure confidentiality, integrity and authenticity of document or information over cloud storage and in addition, there must be some mechanism that helps users to know fast encryption algorithm of their Video Files to be stored in cloud and fast decryption of same Video Files from cloud to their devices.

Therefore we must investigates Conventional algorithm's efficiency over cloud in terms encryption time, decryption time, key sizes, best browser, best operating system,throughput,avalanchee effect, memory utilisation etc.

In this Paper, we will analyse the performance cryptic of various block cipher SKC algorithms to find more efficient symmetric block cipher algorithm for video files in the term of encipherment and decipherment time at different settings like variable file sizes with fixed key sizes, variable file sizes with variable key size, Fixed file sizes with fixed key size and Fixed file sizes with variable key sizes.

II. RELATED WORK

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 [1].

Because in cloud storages, storage providers have full control and cloud users have always fear of losing data in cloud so it has been seen that still users refrains to migrate their confidential data in the cloud. Security of outsourced data is a great challenge. The major requirement for achieving security in outsourced databases are confidentiality, privacy, integrity, availability [2, 3].
Cryptography is first step towards the security of the sensitive information of data owners in cloud storage [4].

Corresponding Author: A Sharma,
Department of Computer Science, BU, Bhopal- India

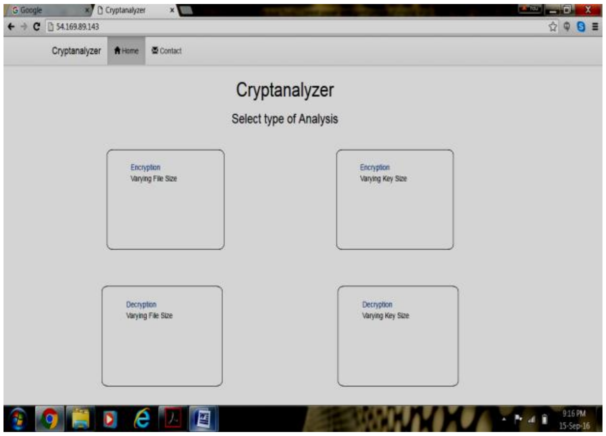
Various Cryptographic algorithms has been introduced from time to time to encrypt the data and mainly it has been seen that AES, 3DES, RC6, Twofish and Blowfish has been used for security purpose.[5]

DES had introduced the Data Encryption standard (DES) in 1977and most widely used Encryption and Decryption scheme till the introduction of Advanced Encryption Standard (AES) in 2001.in DES, data is encrypted in 64-bit blocks using 56-bit key transformed from 64-bit key. In case of Triple-DES, instead of one key, two keys have been used,the first key is used to convert a plaintext message into cipher text and the second key is used to decrypt the encrypted message. Since second key is different from first one, so output is not the plaintext. Therefore, the twice-scrambled message is then encrypted again with the first key to yield the final cipher text. This three-step procedure is called triple-DES.Triple-DES is just DES done three times with two keys used in a particular order [6, 7,8].

AES has captured the market because of aging Data Encryption Standard (DES) which was vulnerable to brute-force attacks.AES consist of three block ciphers, AES-128, AES-192 and AES-256.Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits, respectively. Depending upon the key length number of rounds differs [9, 10, 11]. In [12], a tool designed for comparison of performance of DES, 3DES, Blowfish and Two Fish Cryptosystem using SGcrypter has been presented. The performance has been compared with variable input text size and key size. However, no analysis has been done on other file formats and popular algorithm that is currently being used in cloud. In [13], the theoretical background of symmetric algorithm and its scope for Time variant perspective has been discussed. The paper presents one schemes based on Fibonacci-Q matrix.In [14], the trend of increasing key size has been supported by Automatic variable key with Optimal Key Size. In [15], Various Approaches towards Crypt-analysis have been suggested for testing strength of symmetric cryptosystem. In [16], the specialized class of algorithms for analysis of cipher text Cryptic Mining algorithm in case of Automatic Variable Key Based Cryptosystem has been presented. In [17, 18], Variable key for shorter size has been realization with Fibo-Q based Symmetric Cryptosystem. In [16], the auditing of symmetric key based cryptosystem has been analyzed by Association rule on Parameterized Automatic Variable Key based Symmetric Cryptosystem. In [19], another strategy of symmetric key based cryptosystem using location based information on sparse approach is suggested.

III. EXPERIMENTAL SET UP

Among the existing symmetric key algorithms, choosing much efficient symmetric key cryptographic encryption and decryption technique has been an issue. To choose the best SKC (symmetric key cryptographic) algorithm from a list of symmetric key encryption and decryption algorithms like AES, Blowfish and DES algorithms, we need to find encryption time and decryption time first to get the best out of them.



Cryptanalyzer

Select type of Analysis

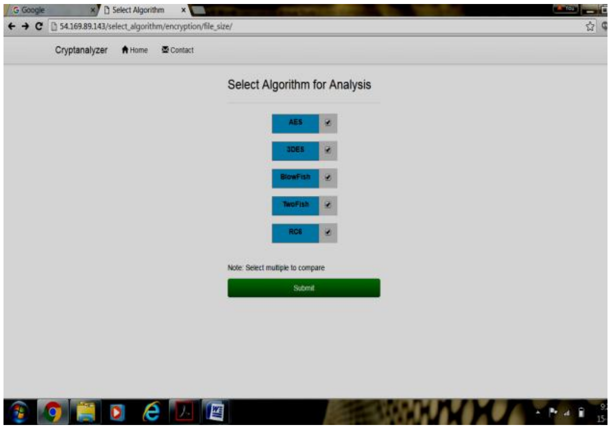
Encryption
Varying File Size

Encryption
Varying Key Size

Decryption
Varying File Size

Decryption
Varying Key Size

Fig.1a. Home Screen of Crypto Tool

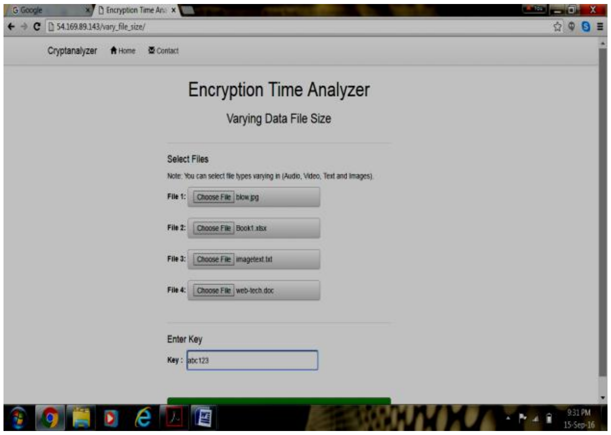


Select Algorithm for Analysis

AES ☑
3DES ☑
BlowFish ☑
TwoFish ☑
RC6 ☑

Note: Select multiple to compare

Fig.1b. Choice of algorithm for comparison



Encryption Time Analyzer

Varying Data File Size

Select Files

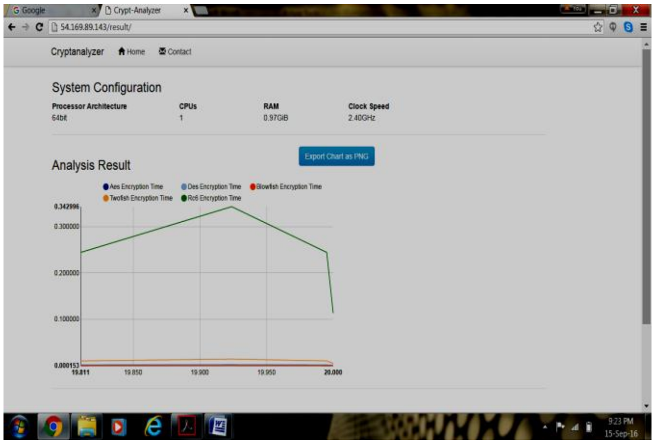
Note: You can select file types varying in (Audio, Video, Text and Images).

File 1: Choose File blow.jpg
File 2: Choose File Book1.xlsx
File 3: Choose File imagetext.txt
File 4: Choose File web-tech.doc

Enter Key

Key : abc123

Fig1c. Types of files for Encryption Time Analyzer



System Configuration

Processor Architecture	CPUs	RAM	Clock Speed
64bit	1	0.97GiB	2.40GHz

Analysis Result

Fig.1d. Plot of performance of Encryption time

We may analyze SKC encryption and decryption algorithms using the web application of Cloud Crypter, which provides actual statistics generated during encryption or decryption in several cases.

Category I: Encryption of Video Files of variable sizes with fixed key.

Category II: Decryption of Video Files of variable sizes with fixed key.

Category III: Encryption of Video Files of fixed size with Variable key sizes.

Category IV: Decryption of Video Files of fixed size with Variable key sizes.

For first category, input files supplied to above tool varies with size of Video Files with fixed key size and corresponding execution time for encryption has been recorded accordingly. The result obtained has been presented in Table 2.1a and demonstrated in figure Fig 2.1a.In second category focus is given on decryption time. For second category with the same input files supplied in category 1 to above tool varies with size of Video Files and corresponding execution time for decryption has been monitored accordingly. The result obtained has been presented in Table 2.1b and demonstrated in figure 2.1b.The performance has been analyzed for all sort of symmetric algorithms that are available and used in commercial product.

For third category with the same input file (any one) supplied in category 1 to above tool varies with size of key Files and corresponding execution time for encryption has been monitored accordingly. The result obtained has been presented in Table 2.1c and demonstrated in figure 2.1c.The performance has been analyzed for all sort of symmetric algorithms that are available and used in commercial product.

For fourth category with the same the same input file (any one) supplied in category 1 to above tool varies with size of key Files and corresponding execution time for decryption has been monitored accordingly. The result obtained has been presented in Table 2.1d and demonstrated in figure 2.1d.

The performance has been analyzed for all sort of symmetric algorithms that are available and used in commercial product.

Explanation and Usage of Cryptic Web Tool Cloud Crypter

For analysis of conventional SKC algorithm's behaviour on variation of key size and file size. We have deployed our Tool in Amazon Cloud Storage. The home screen of Cloud Crypter provides four operations(i)Encryption of different files with Varying key Size(ii) Encryption of different files with fixed key Size(iii) Decryption of different files with varying key Size (iv) Decryption of different files with fixed key.

IV. RESULT AND PERFORMANCE ANALYSIS

In order to analyze the performance of conventional SKC algorithms, various combinations of Video Files of different sizes and keys of different sizes is required. The Cloud Crypter tool has taken a set of Video Files and key with different sizes for this performance analysis.

The different result has been achieved in the form of different graphs and tables for various symmetric key cryptography algorithms are given below.

Performance Analysis of AES, 3DES, AES, 3DES with RC6, Twofish and Blowfish Cryptic Algorithm

In order to investigate the performance of AES, Blowfish and DES algorithms algorithm over various Video Files with variable encryption key size and corresponding time taken to encrypt Video Files is discussed in detail followed by the counter part of Encryption process i.e., decryption of encrypted Video Files (processed with various key lengths) is discussed in later section of this chapter.

Simulation results corresponding to Encryption and Decryption of four Input Video Files of sizes 34.35kb, 13.28kb, 75.01kb, 121.81Kb respectively with fixed key abc121 is depicted in Table 2.1a and Table 2.1b Corresponding Bar-chart representation of performance of AES, 3DES, AES, 3DES with RC6, Twofish and Blowfish algorithm is depicted in Figure 2.1a and Figure 2.1b covering category I&II.

Table 2.1c and 2.1d indicates the Simulation results corresponding to Encryption and Decryption of fixed Video Files file of 34.35 Kb with variable Key sizes of 8kb, 9kb, 10kb and 11kb resp.

Corresponding Bar Chart representation of performance of AES, Blowfish and DES algorithms is depicted in Figure 2.1c and Figure 2.1d covering category III&IV.The Comparative performance of AES, Blowfish and DES algorithms over Video Files of fixed size and variable sizes along with variable fixed Encryption /Decryption keys and variable Encryption /Decryption keys have been investigated and corresponding Encryption/Decryption time taken to generate encrypted/Decrypted Video Files is discussed in this section in great details.

Table 2.1a and 2.1b shows Encryption/Decryption time taken by all algorithms discussed above with variable Video Files and fixed key and Table 1.1c and 1.1d shows Encryption/Decryption time taken by all algorithms discussed above with fixed Video Files File and Variable key Sizes.

Here simulation results corresponding to four Input Video Files 13.28kb, 34.35kb, 75.01kb, 121.81Kb with fixed key of .008Kb is represented by fig 2.1a and fig 2.1b respectively.

Table 2.1c and 2.1d shows Encryption/Decryption time taken by all algorithms discussed above with fixed Video Files

of size 13.28Kb and variable Key sizes of 8kb, 9kb, 10kb and 11kb and Table 2.1c and 2.1d shows Encryption/Decryption time taken by all algorithms discussed above with fixed Video Files File and Variable key Sizes.

Here simulation results corresponding to four Key sizes of 8kb, 9kb, 10kb and 11kb with fixed Video Files of size 13.28Kb is represented by fig 2.1c and fig 2.1d respectively.

Table 2.1a: Encryption Time Taken by algorithms with fixed key of file size 8Kb.

File Size	3DES	blowfish	AES
34.35KB	0.004780	0.001059	0.000785
63.28KB	0.008714	0.001902	0.001309
75.01KB	0.010430	0.002316	0.001618
121.81KB	0.017116	0.003647	0.002646

Table2.1b: Decryption Time Taken by algorithms with fixed key of file size 8Kb.

File Size	3DES	blowfish	AES
34.35KB	0.004787	0.001014	0.0000742
63.28KB	0.008754	0.001857	0.0001365
75.01KB	0.010467	0.002171	0.0001617
121.81KB	0.017150	0.003120	0.0002621

Table 2.1c: Encryption Time Taken by algorithms with fixed Video Files of 34.35Kb with variable key Files.

File Size	3DES	blowfish	AES
8byte	0.004780	0.0001078	0.000733
9byte	0.004771	0.0001011	0.000745
10byte	0.004730	0.0001074	0.000756
11byte	0.004795	0.0001018	0.000745

Table 2.1d: Decryption Time Taken by algorithms with fixed Video Files of 34.35Kb with variable key Files

Key Size	3DES	blowfish	AES
8byte	0.004747	0.001001	0.00758
9byte	0.004785	0.001013	0.00746
10byte	0.004815	0.001017	0.00738
11byte	0.004785	0.001013	0.00741

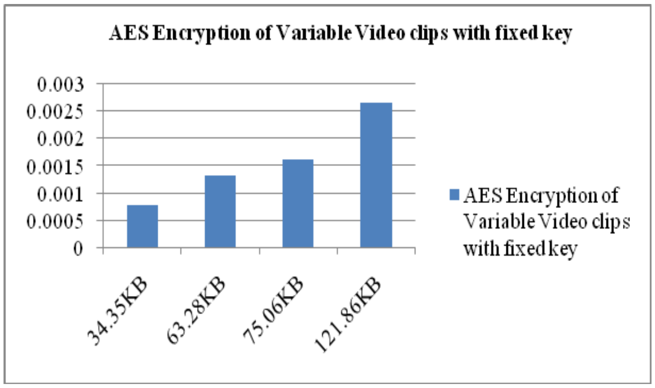


Fig2a: AES Encryption of Variable Video clips with fixed key

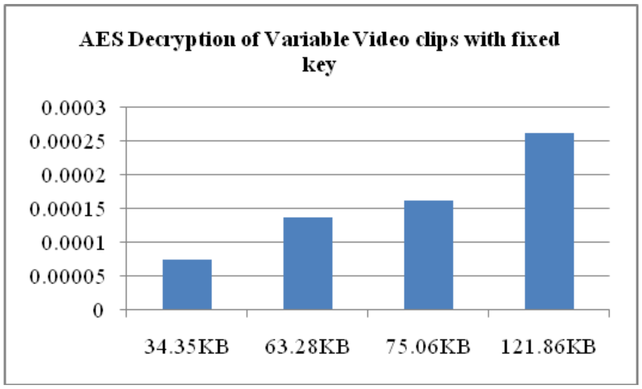


Fig2b: AES Decryption of Variable Video clips with fixed key

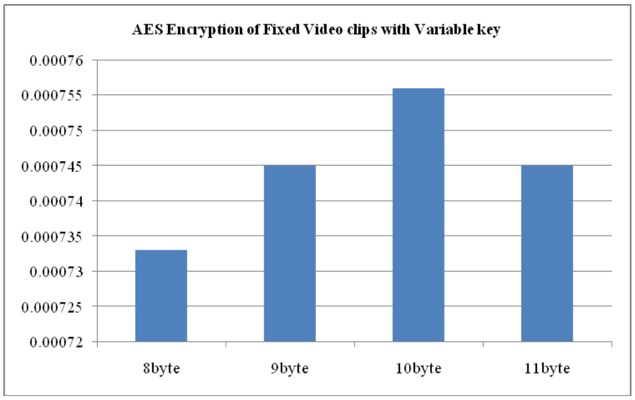


Fig2c:AES Encryption of Fixed Video clips with Variable key

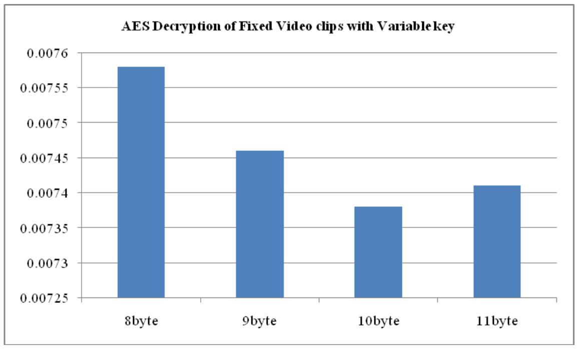


Fig2d:AES decryption of Fixed Video clips with Variable key

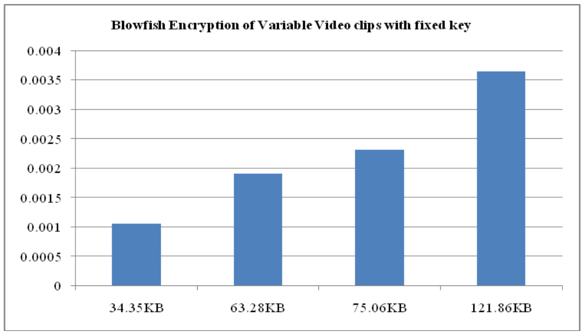


Fig3a: Blowfish Encryption of Variable Video clips with Fixed key

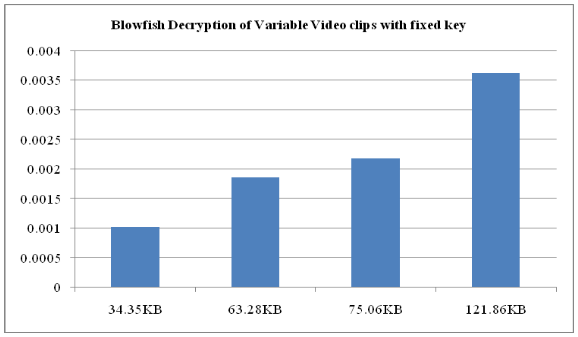


Fig3b: Blowfish Decryption of Variable Video clips with Fixed key

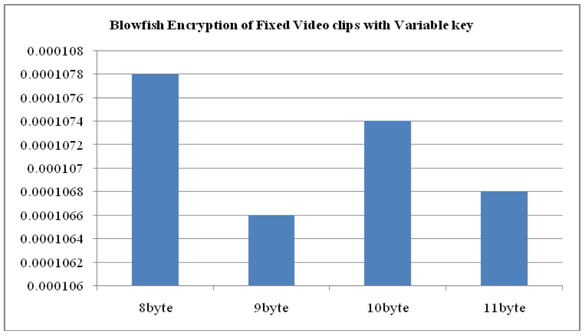


Fig3c: Blowfish Encryption of Fixed Video clips with Variable key

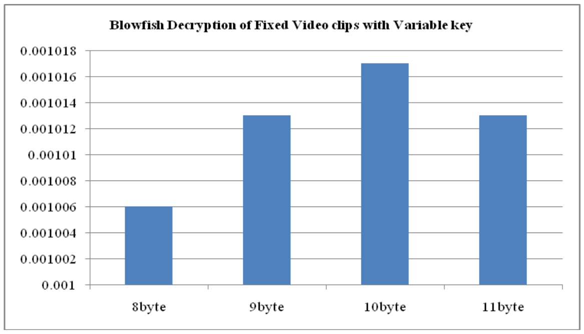


Fig3d: Blowfish decryption of Fixed Video clips Variable key

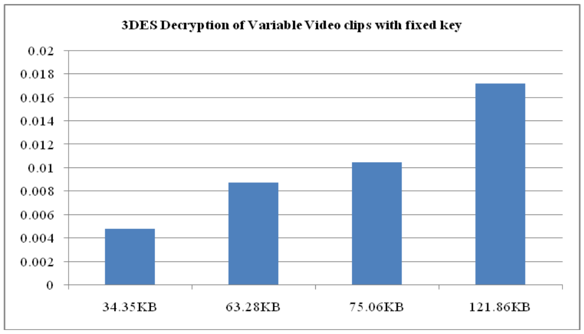


Fig4a**:** 3DES Encryption of Variable Video clips with Fixed key

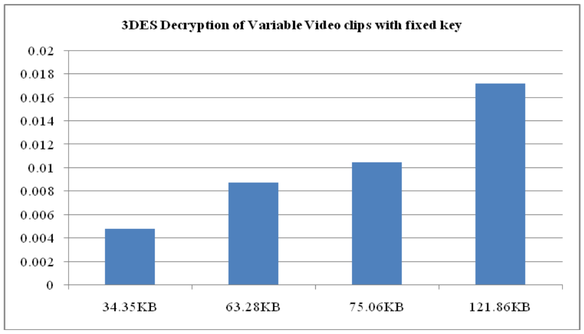


Fig4b: 4DES Decryption of Variable Video clips with Fixed key.

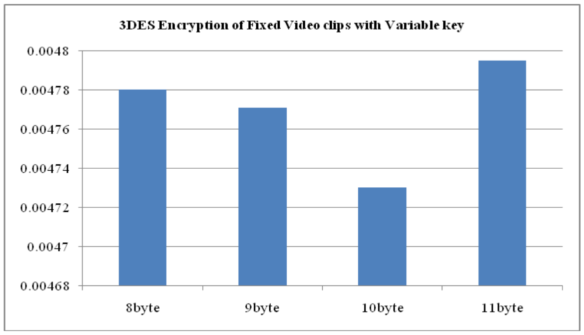


Fig4c: 3DES Encryption of Fixed Video clips with Variable key

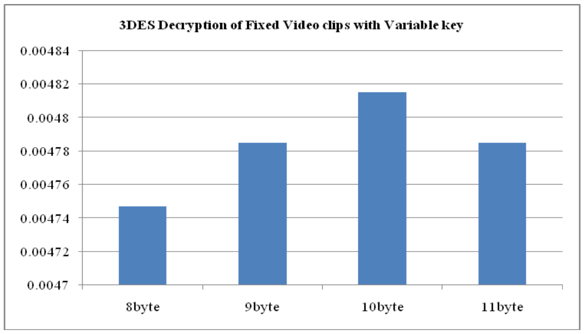


Fig4d: 3DES Decryption of Fixed Video clips with Variable key

V. OBSERVATION AND CONCLUSION

Careful examination of experimental works reveals the following.

In case of Encryption Time Taken by algorithms for variable video files with fixed key of file size 8Kb ,Among AES, Blowfish and 3DES, AES and Blowfish take very less time in comparison to 3DES, RC6 and others algorithms and encryption time in blowfish is almost 7-9 times much compared to AES and Blowfish.

In case of Decryption Time Taken by algorithms for variable video files with fixed key of file size 8Kb, Among AES, Blowfish and 3DES, AES and Blowfish take very less time in comparison to 3DES, RC6 and others algorithms and encryption time in blowfish is almost 7-9 times much compared to AES and Blowfish but all algorithms takes little less than encryption time taken by these algorithms.

In case of Encryption Time Taken by algorithms for fixed video clips with variable key, Among AES, Blowfish and 3DES, again AES and Blowfish take very less time in comparison to 3DES, RC6 and others algorithms and encryption time in blowfish is almost 7 times much compared to AES and Blowfish but all algorithms takes little less than encryption time taken by these algorithms and also it has been seen with fixed video file size and variable keys encryption time is not varying too much and it is almost same with variable key file sizes. This is because we have take file sizes of 9-12kb only. Therefore, impact of variable key on fixed file has little impact on encryption time.

In case of Decryption Time Taken by algorithms for fixed video clips with variable key, Among AES, Blowfish and 3DES , again AES and Blowfish take very less time in comparison to 3DES, RC6 and others algorithms and decryption time in blowfish is almost 7 times much compared to AES and Blowfish but all algorithms takes little less than decryption time taken by these algorithms and also it has been seen with fixed video file size and variable keys encryption time is not varying too much and it is almost same with variable key file sizes. This is because we have take file sizes of 9-12kb only. Therefore, impact of variable key on fixed file has little impact on decryption time.

The result shows that AES must be preferred over the other Symmetric algorithm in terms of encryption and decryption time for video files in cloud. However, when we look into the parameters like throughput and Memory consumption then Blowfish must be preferred over AES.

In future, we must look into area where improvement can be done in AES working so that it can be preferred on most of the parameters for cloud.

REFERENCES

[1] 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, pp.13-16, 2013.

[2] Shivlal Mewada, Umesh Kumar Singh and Pradeep Sharma, "*Security Enhancement in Cloud Computing (CC)"*, International Journal of Scientific Research in Computer Science and Engineering, Vol.1, Issue.1, pp.31-37, 2013.

[3] Shivlal Mewada, UK Singh, Pradeep Sharma, "*Security Based Model for Cloud Computing",* International Journal of Computer Networks and Wireless Communications, Vol.1, No.1, pp.13-19, 2011.

[4] Aarti Shrivastava, Pradeep Sharma, Shivlal Mewada, "*Two Level Security Algorithm of Data in Cloud Computing*", UDGAM VIGYATI, Vol 2, pp.188-195, 2015.

[5] 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, pp.23-30, 2016.

[6] CH. Meyer, SM. Matyas, "*Cryptography: A New Dimension in Computer Data Security*", John Wiley & Sons, NewYork, pp.1-640, 1982.

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

[1] 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, pp.1-450, 1989.

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

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

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

[12] Shaligram Prajapat, Gaurav Parmar, R.S.Thakur, "*Towards investigation of efficient Cryptosystem using Sgcrypter*", Special Issue of International Journal of Applied Engineering and Research (IJAER), Vol. 10, Issue.79, pp. 853-858, 2015.

[13] S. Prajapat, D. Rajput, Ramjeevan Singh Thakur, "*Time variant approach towards symmetric key",* proceedings of IEEE Science and Information Conference (SAI), London, pp.398-405, 2013.

[14] Prajapat, Shaligram, Ramjeevan Singh Thakur, "*Optimal Key Size of the AVK for Symmetric Key Encryption*", in Covenant Journal of Information & Communication Technology, Vol.3, Issue.2, pp. 71-81. 2015.

[15] Prajapat, Shaligram, Ramjeevan Singh Thakur, *"Various Approaches towards Crypt-analysis"*, International Journal of Computer Applications, Vol. 127, Issue.14, pp. 15-24, 2015.

[16] S. Prajapat, RS. Thakur, "*Cryptic Mining for Automatic Variable Key Based Cryptosystem*", Elsevier Procedia Computer Science, Vol. 78, Issue.78C, pp. 199-209, 2016.

[17] S. Prajapat, RS. Thakur, "*Realization of information exchange with Fibo-Q based Symmetric Cryptosystem*", International Journal of Computer Science and Information Security, Vol 14(2), pp. 216-223, 2016.

[18] S. Prajapat, A. Jain, RS. Thakur, "*A Novel Approach For Information Security with Automatic Variable Key Using Fibonacci Q-Matrix*", IJCCT, Vol.3. Issue.3, pp.54-57, 2012.

[19] A.N.A. El-Sheikh, A.A. Rashed, "*New Approach in Key Generation and Expansion in Rijndael Algorithm*", International Arab Journal of Information Technology, Vol..3, no. 1, pp. 35-41, 2006.

Authors Profile

Mr. Ashok Sharma pursed Bachelor of Science from University of Jammu,Jammu in 1998 and Master of Science from Jiwaji University Gwalior in year 2001. He is currently pursuing Ph.D. and He is a member of IEEE &life Member of CRSI India . He has 15 years of teaching experience..

Dr RamJeevan Singh Thakur is currently working as Associate Professor in Department of Computer Application,MANIT Bhopal. He is member of IEEE,CSI,ACM and He is borad Member of Varous reputed orgnaistaion. He has guided more than 20 PhD Scholars and he has published more than 80 research papers in reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE and his main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education. He has 18 years of teaching experience and 7 years of Research Experience.

Dr. Shailesh Jaloree is currently working as Professor&Head,Department of Mathematics,SATI Vidisha,MP. He has guided more than 20 PhD Scholars and he has published more than 90 research papers in reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE and his main research work focuses on Cryptography Algorithms, Modern Algebra, Data Mining, IoT and Computational Intelligence based education. He has 25 years of teaching experience.