International Journal of Scientific Research in ______________________________ **Research Paper**
Computer Science and Engineering
Vol.4, Issue.5, pp.5-11, October (2016) **E-ISSN:**2320-7639

Investigation of Efficient Cryptic Algorithm for image files Encryption in Cloud

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

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

Corresponding Author: ashoksharmamca@gmail.com

Available online at: www.isroset.org

Received: Sep/12/2016, Revised: Sep/20/2016, Accepted: Oct/19/2016, Published: Oct/30/2016

Abstract- *Wi*th the increasing demand of Cloud based resources, the customers have been attracted to the various offerings of cloud computing and mainly it has been seen that the Cloud storages have been centre of attraction because of free limited storage for users. Customers are moving their documents into cloud storages because of various options in cloud storages. We are using various mobile based apps to store images in our system but due to limited storage capacity of our system we prefer cloud storages for storing different files specially images. The image files include files of various formats like JPG Image Files, GIF Images, JPEG Files etc. The image 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 for fast encryption of their image to be stored in cloud and fast decryption of same image from cloud to their devices. Since the service level, agreements are very strong and there is no fear to keep the data in cloud because of strong SLA implementation policies. Therefore, we must investigate Conventional algorithm's efficiency over cloud in terms encryption time, decryption time, key sizes. In this paper we will analyse the performance for exchange of Images with various block cipher SKC algorithms specially 3DES, AES and Blowfish to find more efficient symmetric block cipher algorithm 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.

Index Terms -Cloud Computing, Cryptography, Encryption, Crypter Tool, Decryption, encipherment and decipherment

I. INTRODUCTION

With the birth of cloud based computing various issues have been developed and researchers have suggested various solutions of these problems. One of issues among these was data security in cloud. Since we are using various offerings of cloud computing which ranges from processing capabilities to storages capabilities in cloud.For securing data in cloud, cryptography has played an excellent role. Cryptography can be applied at three sections, one is at cloud provider's site which is treated as insecure, second option is to implement encryption at third party and lastly, implementation of encryption at client end.

If we apply encryption to massive data at client end, it means there is no need to use cloud storage. We move to cloud storages and third party encryption is again complicated because of massive data transfers from client to third party for encryption and then back. But due to complexities of processing massive data at client end and third party transferring massive data to cloud, encryption at cloud is easy but due to security same is avoided by customers. With the birth of strong service level agreements (SLA's) Customer's grievance has been resolved up to extent and now because of strong implementation of SLA's, customers are encouraged to use encryption at cloud end without fear. Now an issue of selection of appropriate algorithm for encryption of different format of documents in cloud is required.

Therefore we must investigates Conventional algorithm's efficiency over cloud in terms encryption time, decryption time, key sizes, best operating system for encrypting different format of documents.

In this Paper, we will analyse the performance for encryption of image Files with various block cipher SKC algorithms to find more efficient symmetric block cipher algorithm in the term of decipherment 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

Nowadays, massive information is migrating from local machine and storages to cloud based storages because of various offerings by cloud provider. Due to exponential Growth of social networking, variety of information contents especially images are widely used in different processes. Therefore, the security of image data from unauthorized uses is important. Conventional Image encryption schemes does information hiding and making it unreadable and prevents from hacker or eavesdropper (including server administrators and others) that have access to these contents or any other type of transmitted information through Social media.

Traditional Image-Cryptic algorithms get the pixels of the input image to transform into cryptic image in variety of ways. The comparative analysis of these schemes is essential to explore the Faster encryption time such that encrypted image is exchanged faster to the person. Perfection in the transformation back into image after deciphering 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].

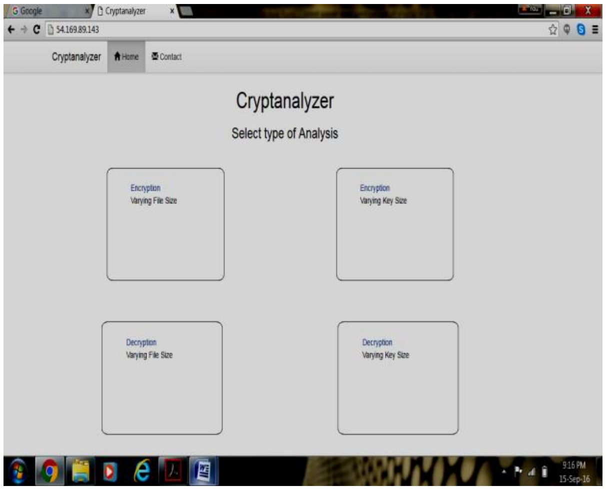
Because in cloud storages, storage providers have full control and user have always fear of losing data in cloud so it has been seen that till users refrains to migrate their confidential data in the cloud. Security of outsourced data is a great challenge. The major requirement for achieving security in outsourced databases are confidentiality, privacy, integrity, availability [4,5,6,7].

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.[7,8,9,10,11,12,13,14,15,16,17]

We have assumed that strong service level agreements within cloud users and cloud providers, encouraged the adoption of cloud based encryption.

III. EXPERIMENTAL SET UP

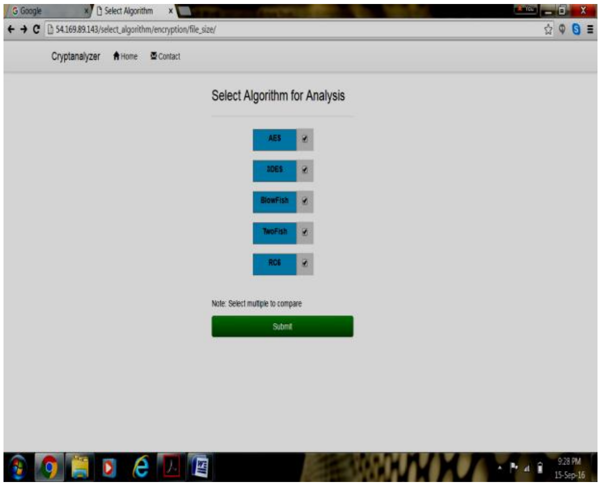
Among the existing symmetric key algorithms, choosing much efficient symmetric key cryptographic encryption and decryption technique has been an issue. To choose the best SKC (symmetric key cryptographic) algorithm from a list of symmetric key encryption and decryption algorithms like AES, Blowfish and 3DES algorithms, we need to find encryption time and decryption time first to get the best out of them.


54.169.89.143

Cryptanalyzer

Select type of Analysis

Fig.1a. Home Screen of Crypto Tool

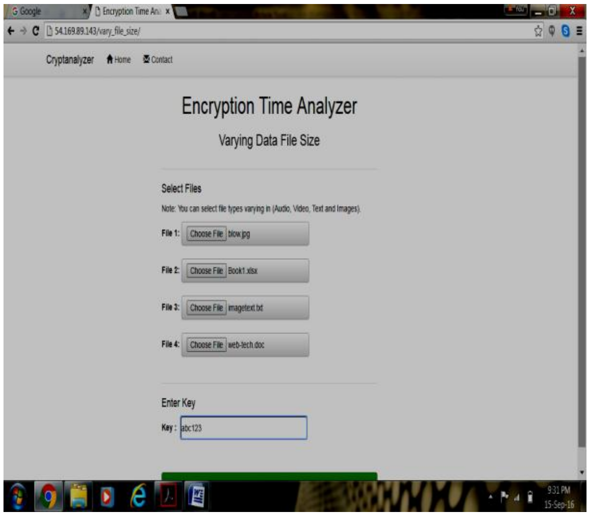

54.169.89.143/select_algorithm/encryption/file_size/

Select Algorithm for Analysis

AES ☑
3DES ☑
BlowFish ☑
TwoFish ☑
RC6 ☑

Note: Select multiple to compare

Fig.1b. Choice of algorithm for comparison


54.169.89.143/vary_file_size/

Encryption Time Analyzer

Varying Data File Size

Select Files

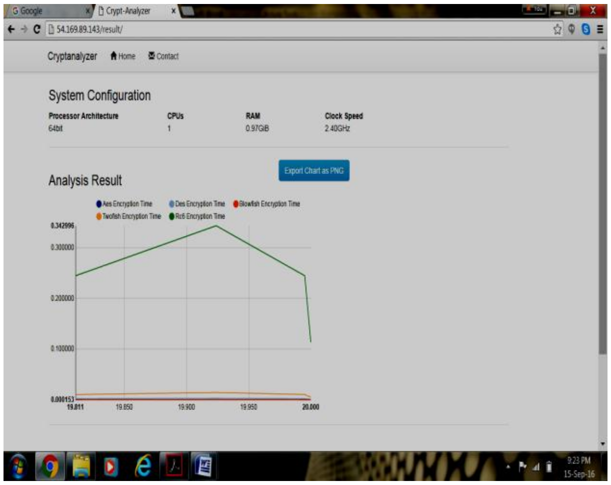
Note: You can select file types varying in (Audio, Video, Text and Images).

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 are investigating best cipher using cloud Crypter tool, which provides actual statistics generated during encryption or decryption in several cases.
Category I: Encryption of image Files of variable sizes with fixed key.
Category II: Decryption of image Files of variable sizes with fixed key.
Category III: Encryption of Image Files of fixed size with Variable key sizes.
Category IV: Decryption of Image Files of fixed size with Variable key sizes.

For first category, input files supplied to above tool varies with size of Image 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 Image 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.

IV. RESULT AND PERFORMANCE ANALYSIS

In order to analyze the performance of conventional SKC algorithms, various combinations of Image Files of different sizes and keys of different sizes is required. The Cloud Crypter tool has taken a set of Image Files and key with different sizes for this performance analysis. The different results achieved in the form of different graphs and tables for various symmetric key cryptography algorithms are given below. In order to investigate the performance of AES, Blowfish and DES algorithms algorithm over various Image Files with variable encryption key size and corresponding time taken to encrypt Image Files is discussed in detail followed by the counter part of Encryption process i.e., decryption of encrypted Image Files (processed with various key lengths) is discussed in later section of this chapter.

Simulation results corresponding to Encryption and Decryption of four Input Image Files of sizes 19kb, 20kb, 225Kb and 242Kb respectively with fixed key is depicted in Table 2.1a and Table 2.1b Corresponding Bar-chart representation of performance of AES, 3DES 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 Image Files of 19 Kb with variable Key sizes of.008kb, .009kb, .0010kb and .0011kb respectively.

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 3DES algorithms over Image 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 Image 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 Image Files and fixed key and Table 1.1c and 1.1d shows Encryption/Decryption time taken by all algorithms discussed above with fixed Image Files File and Variable key Sizes.

Here simulation results corresponding to four Input Image Files 19kb, 20kb, 225Kb and 242Kb respectively 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 Image Files of size 13.28Kb and Key sizes of.008kb, .009kb, .0010kb and .0011kb respectively. in Table 2.1c and 2.1d shows Encryption/Decryption time taken by all algorithms discussed above with fixed Image Files File and Variable key Sizes.

Here simulation results corresponding to four Key sizes of 8kb, 9kb, 10kb and 11kb with fixed Image Files of size 19Kb 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 .008Kb.

File Size	3DES	blowfish	AES
20kb	0.001987	0.00456	0.000435
19kb	0.002731	0.00634	0.000327
225kb	0.030305	0.006738	0.004665
242kb	0.032781	0.007266	0.005039

Table2.1b: Decryption Time Taken by algorithms with fixed key of file size .008Kb.

File Size	3DES	blowfish	AES
20kb	0.002017	0.000432	0.000318
19kb	0.002810	0.000598	0.000455
225kb	0.030604	0.006432	0.004699
242kb	0.033052	0.006976	0.005122

Table 2.1c: Encryption Time Taken by algorithms with fixed Image Files of 19Kb with variable key Files.

File Size	3DES	blowfish	AES
.008kb	0.002011	0.000463	0.000321
.009kb	0.001947	0.000472	0.000319
.0010kb	0.002004	0.000458	0.000318
.0011kb	0.002014	0.000459	0.000330

Table 2.1d: Decryption Time Taken by algorithms with fixed Image Files of 19Kb with variable key Files

Key Size	3DES	blowfish	AES
.008kb	0.001981	0.000429	0.000324
.009kb	0.002007	0.00043	0.000318
.0010kb	0.001982	0.000428	0.000315
.0011kb	0.001984	0.000425	0.000319

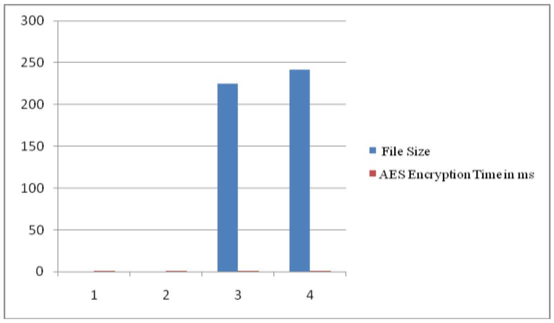


Fig2a: AES Encryption of Variable Image clips with fixed key

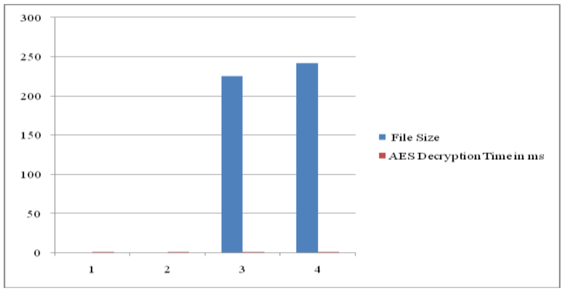


Fig2b: AES Decryption of Variable Image clips with fixed key

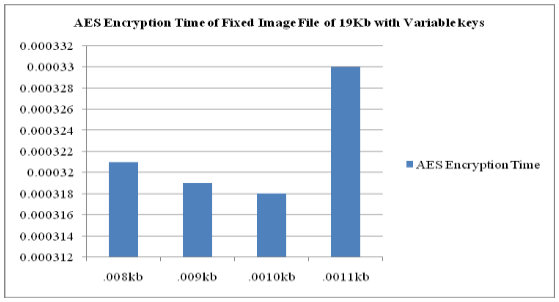


Fig2c:AES Encryption of Fixed Image clips with Variable key

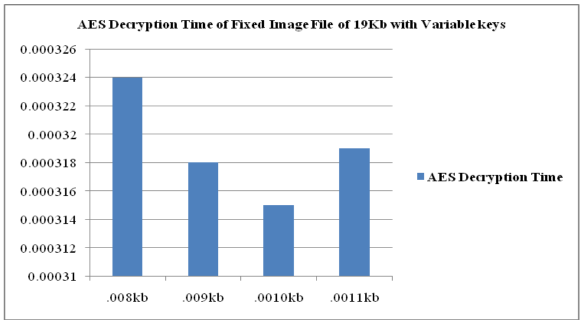


Fig2d:AES decryption of Fixed Image clips with Variable key

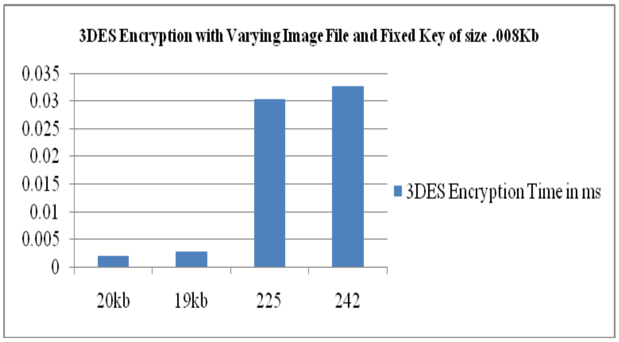


Fig3a 3DES Encryption of Variable Image clips with Fixed key

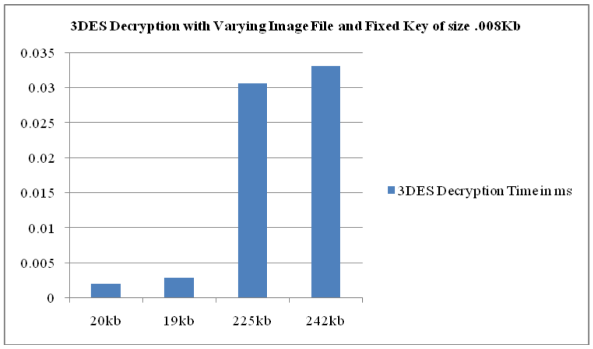


Fig3b: 3DES Decryption of Variable Image clips with Fixed key

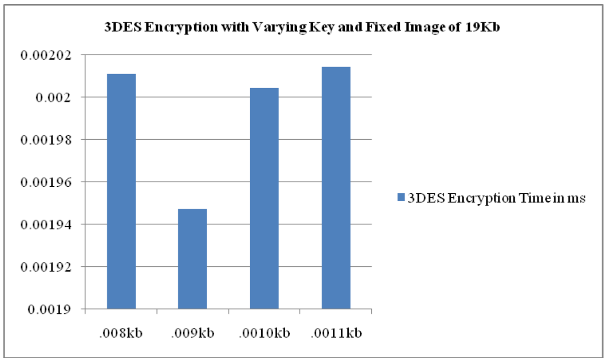


Fig3c: 3DES Encryption of Fixed Image clips with Variable key

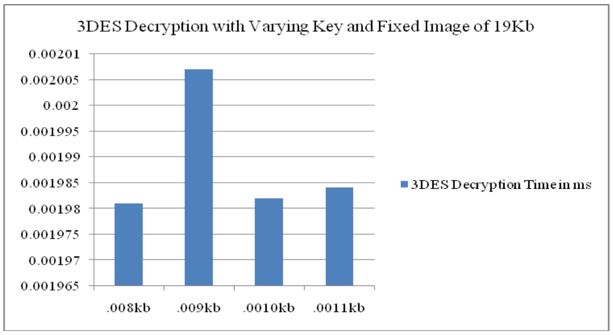


Fig3d: 3DES decryption of Fixed Image clips Variable key

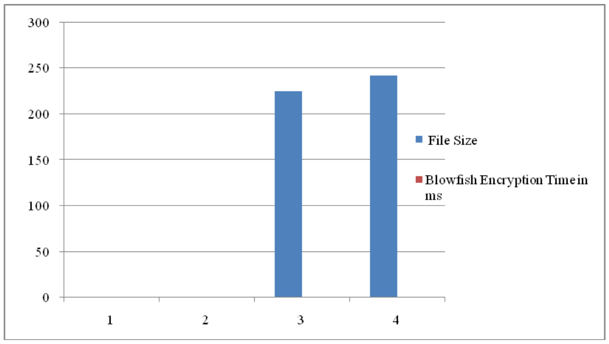


Fig4a**:** Blowfish Encryption of Variable Image clips with Fixed key.

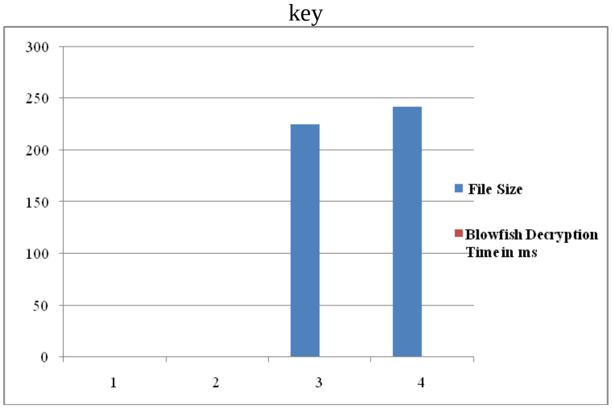


Fig4b: Blowfish Decryption of Variable Image clips with Fixed key.

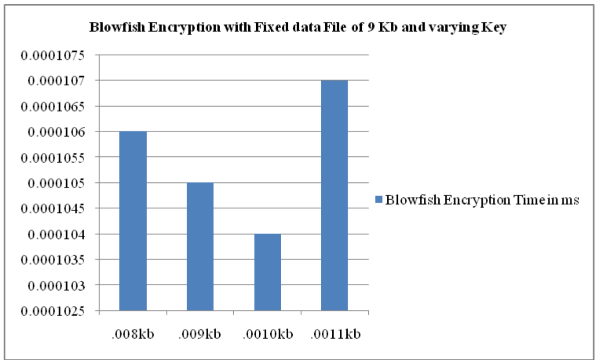


Fig4c: Blowfish Encryption of Fixed Image clips with Variable key

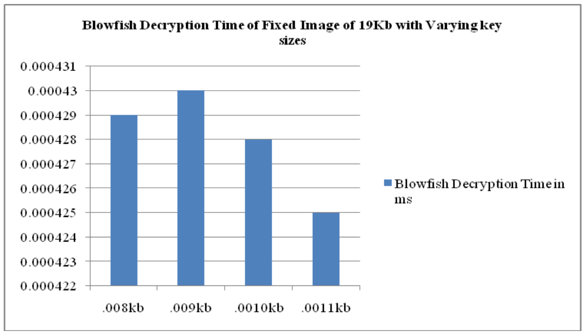


Fig4d: Blowfish Decryption of Fixed Image clips with Variable key

V. OBSERVATION AND CONCLUSION

After investigation of experimental work, we have observed that in case of Encryption Time Taken by algorithms for variable image files with fixed key of file size .008Kb,AES takes less time than Blowfish and 3DES.anyhow the time taken by AES and Blowfish is somehow comparable but 3DES is taking almost 5-6 times much encryption time compared to AES and Blowfish .We have found that with the increase in file size, encryption time also increases.

In case of Decryption Time Taken by algorithms for variable image files with fixed key of file size .008Kb, Among AES, Blowfish and 3DES, AES and Blowfish take very less time in comparison to 3DES and others algorithms and encryption time in 3DES is almost 6-7 times much compared to AES and Blowfish. We have found that with the increase in file size, encryption time also increases. In case of encryption Time Taken by algorithms for fixed image clips with variable key, AES and Blowfish take very less time in comparison to 3DES and encryption time in 3DES is almost 5 times much compared to AES and Blowfish. it has been seen with fixed image file size and variable keys 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 Taken by algorithms for fixed image clips with variable key, again AES and Blowfish takes almost very less time than 3DES but decryption time in 3DES is almost 6 times much compared to AES and also it has been seen that with fixed image 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 must be preferred over the encryption and decryption of image files in terms of encryption and decryption time in cloud. However, when we look into the parameters like throughput and Memory consumption then Blowfish, must be preferred over AES.

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, pp.23-30, 2016.

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

[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, pp.13-16, 2013.

[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, pp.1-5, 2016.

[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, pp.663–666, 2016.

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

[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, pp.1-450, 1989.

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

[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, pp.105-110, 2016.

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

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

[12] 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.

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

[14] Prajapat, Shaligram, Ramjeevan Singh Thakur, “*Cryptic Mining for Automatic Variable Key Based Cryptosystem*”, Elsevier Procedia Computer Science, Vol.78, Issue.78C, pp. 199-209, 2016.

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

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

[17] Prajapat, Shaligram, Jain A. Ramjeevan Singh Thakur, *“A Novel Approach For Information Security with Automatic Variable Key Using Fibonacci Q-Matrix*”, IJCCT, Vol-3(3), 2012, p.p. No. 54-57, 2012.

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.

Prof.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 35 years of teaching experience.