ISSN 2347 - 3983
Volume 8. No. 4, April 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter71842020.pdf
https://doi.org/10.30534/ijeter/2020/71842020

Encrypting and decrypting different files over different algorithm on Cloud Platform

M.Robinson Joel[1], V.Ebenezer[2], M.Navaneethakrishnan[3], N.Karthik[4]
[1]Ponnaiyah Ramajayam Institute of Science and Technology, India, joelnazareth@gmail.com
[2]Karunya Institute of Technology and Sciences, India, ebenezer88@gmail.com
[3]St.Joseph College of Engineering, India, navanee81@gmail.com
[4]Karunya Institute of Technology and Sciences, India, nkarthikapce@gmail.com

ABSTRACT
Now-a-day applications like e-banking, online marketing, medical data application, etc., are attacked by many malware. Especially in cloud computing, the data security is the most important aspects and the speed is also taken into account. This internet turns into the main intermediate between machine and mankind for smiles to tears. Similarly, the online transaction becomes the main event in human life for all-purpose like purchase vegetables to diamonds. In our paper, we plan to show the security and performance of the different security concepts namely AES, Blowfish and Twofish. We can explain the safety factors and security issues of these blowfish, Twofish and AES algorithm. We are going to encrypt variety data types like text file, image file and audio file over the three algorithms and find the speed of encryption. Similarly their performances on different size of input files have been analyzed. It is useful to select the correct algorithm for exact input files to share between the two nodes within time.

Key words : Twofish, AES, Blowfish, Cloud computing, Data Security, Malware.

1. INTRODUCTION

In this new digital era, wishes to withdraw are made online. This internet turns into the main intermediate between machine and mankind for smiles to tears. Similarly, the online transaction becomes the main event in human life for all-purpose like purchase vegetables to diamonds.

Due to the increase in data transferred between systems the intruders also increased. These people make threats to the information in all aspects. To avoid these type of things people starting hiding and encrypting their data in some different ways.Writing secret with the help of science and art is termed as Encryption[1][8]. Figure 1 shows the Encryption and decryption schemes, which convert the plain text to ciphertext and vice versa to the receiver side.

Carlos[2] explained the cloud computing[18][19][23][24] and its demands in his work. In recent years the cloud computing[21][22] became a hotcake for many computational solutions for the knowledge fields.

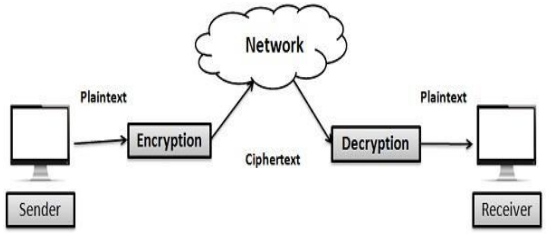

Figure 1: Encryption and Decryption Scheme

In recent scenario computing resources becoming extremely demanding to perform those tasks with acceptable performance. Figure 2[9][20] shows the different cloud storage available in the market.

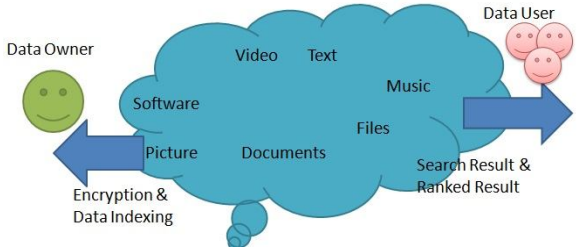

Figure 2: Cloud Storage explained by Robinson and team

2. RELATED WORK

In this section, we discuss the performance of various algorithms and their result obtained. S.Hirani was expressed [3] that among the encryption algorithms AES faster and efficient by applying them some experiments on them. By applying the data for transmission, he found out that there is a difference shown in the performance of different symmetric key schemes. He proposed that AES scheme is better for data transfer. P. Ruangchaijatupon [4] shows that the energy consumption on different machines by the different common symmetric key encryptions algorithms.

In the security domain, the twofish is an important symmetric key block cipher. This twofish has a maximum of 256 bits as key sizes and a maximum of 128 bits as block size. This twofish algorithm, as well as key, can be used for encryption and decryption of the same[5]. S. Z. S. Idrus [6] analysis different web browsers using web programming language and measure the security level. The main aim of the analysis consist of encryption performance of a programming language over a web browser. They conduct some experiment to obtain best result of encryption algorithm versus Web browser.

This Twofish algorithm, as well as key, can be used for encryption and decryption of the same.Blowfish algorithm[7] generally categorised as a symmetric block cipher, planned by Bruce Schneier in 1993[11]. 32 bits to 448 bits variable-length key are used for perfect securing information. Bruce put forward a new configuration with new variable length key of 64-bit block. The main algorithm contains two parts like data encryption part of 16-round Feistel network and key expansion part of at most 448 bits. These bits divided into several subkey arrays of bytes whichs comes totaling 4168 bytes.

Krishnamurthy[10], proposed a method which change the Function F of the Blowfish's Feistel network. This blowfish cryptography also used to convert the plain text to crypto text. They go for Very High Speed Integrated Circuit Hardware Description Language(VHDL) application which show the exact differences in the delay compare to software when implemented encryption and decryption.

In the current population, medical data and patient data are increased rapidly. Anjana Devi[12] proposed an efficient management system for clinical laboratories that secure the patient details and doctors report. For the above needs, Anjana Devi develop laboratories to devise a faster and efficient system which to provide security against cryptic attacks. The proposed system secure the patient data and doctors reports against the patient on the cloud storage with the help of encryption and decryption algorithm. For these two process tey go with twofish algorithm to secure the patients test report and data of the healthcare industry.

Much Aziz Muslim[13] proposed a concept of implementing the twofish algorithm in a communication network for the security of data using library Chilkat. They used an agile method to implement the software which can be implemented as quickly as possible.

Rizky Riyaldhi[14] put forward a novelty method which gives an additional boost to enhance this AES algorithm which also Mix Column transformation happened with S.Box along with Shift Row. They produced a good result of the optimization of around 86%. Also, they show a reduced of 3ms in the timing of optimization and gave improvement as the bytes grows. David [15] proposed the security encryption implementation on Field Programmable Gate Array (FPGA). They used the VHDL language to implement this type of algorithm.

While using the hardwire concept we can't expect the best performance. Since the hardware does not support some sort of it configuration what we are using nowadays. Some time this hardwire also produce best ouitput results compared to programmable coding. The programmer should have the entire knowledge about the hardware where we are going to implement this encryption algorithm[16]. These things led to the changes happened regularly to adjust in the programming codes. But compare with the hardwire products in the market the solution to avoid the cost is to go with the software products. but the number of bits the operating system holds is very important when we design the software. Nowadays the operating systems run on two major bit configuration that is 32bit and 64 bit systems [17].

3. IMPLEMENTATION AND RESULTS

Java was used to implement the scheme with some data. Java is considered platform independent because Java compiler produces byte code rather than machine code for a specific type of hardware - this feature of Java makes sure that the programs will adopt on any platform (with Java interpreter). Thus, the implemented algorithms can be tested on a variety of platforms for comparison purposes.

Cryptography algorithms have some drawbacks while implement them using Java. Java compiler produces an intermediate form code that is byte code which needs interpreter and it does not generate native machine code so the response time is slow. To analysis, the various algorithm in the same language and the same platform will be used to test them without any deviation. For this, we choose Java as our language.

In our work, we perform the performance test on algorithm like AES, blowfish and twofish with different types of inputs. For example, we test the text file, image file and audio file into the above said algorithm and find out the speed of the algorithm. For this we are going test on system with the following configuration like corei3 as processor with speed of 2.87Ghz and 4GB RAM. Figure 3 shows an implementation of AES, Twofish and Blowfish.

We use [8] pearson correlation to find out the coefficient of the performance. Performance of text file with different size are given below. In this paper, different size of text file, audio file and image file have analyzed. Table 1 shows the performance of text file. Figure 4 shows Performance graph of text file. Figure 5 shows an implementation of AES, Twofish and Blowfish on text file. Figure 6 shows Performance graph of image file. Figure 7 shows Performance graph of audio file.

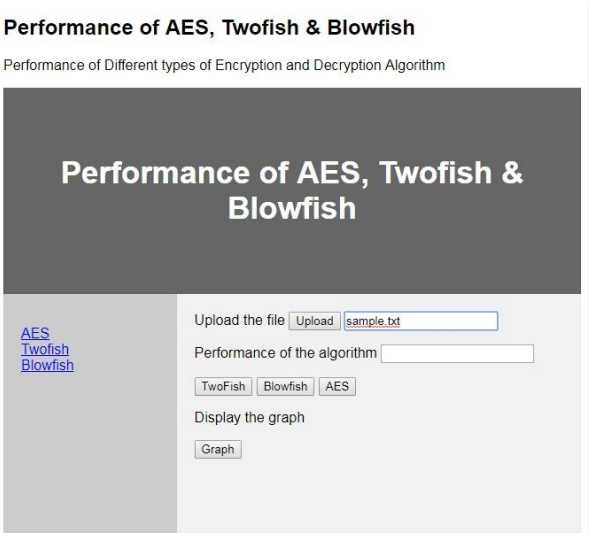

Figure 3: Implementation of AES, Twofish and Blowfish

Table 1: Tabulation of different size of text file performance on different algorithm

Text File	File 1	File 2	File 3	File 4	File 5	File 6	Average Time
Text Size(KB)	1212	1470	1890	2235	6759	8760	3727.50
Two fish	152	174	181	201	431	453	301.83
AES	170	198	201	245	485	512	265.33
Blow fish	168	191	187	237	480	501	294.00

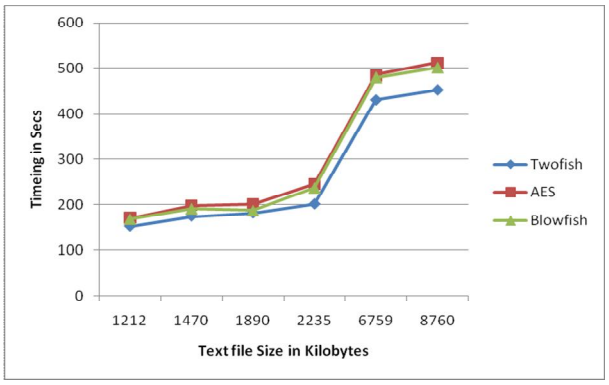

Figure 4: Performance graph for text files

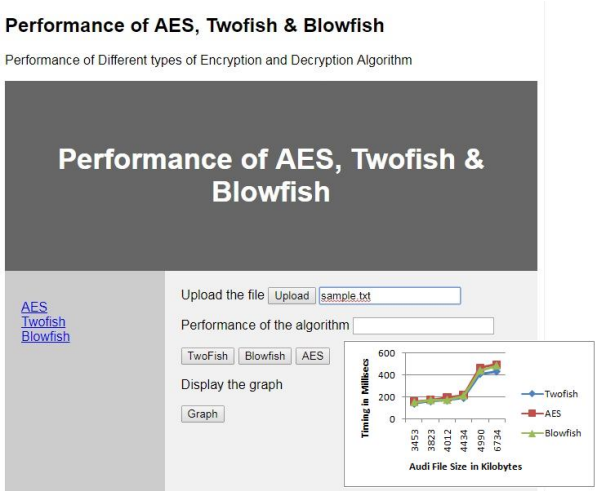

Figure 5: Implementation of AES, Twofish and Blowfish on text file

Table 2 shows the performance of image file. Table 3 shows the performance of audio file.Performance of image file with different size are given below.

Table 2: Tabulation of different size of image file performance on different algorithm

Image File	File 1	File 2	File 3	File 4	File 5	File 6	Average Time
File Size(KB)	21.3	25.4	53.3	112	189	210	101.83
Two fish	87	93	157	297	301	333	211.33
AES	73	83	145	289	311	325	204.33
Blow fish	88	95	160	299	304	337	213.83

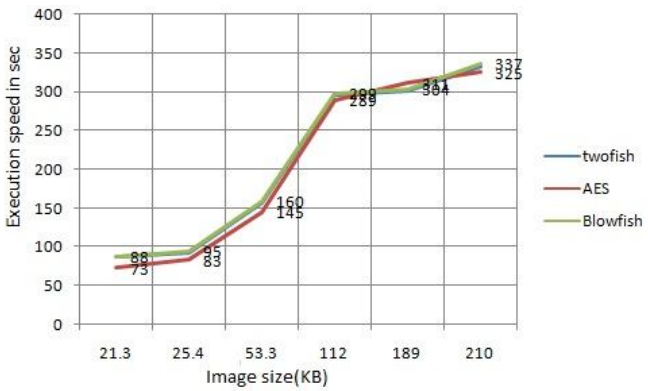

Figure 6: Performance graph for image files

Performance of audio file with different size are given below.

Table 3: Tabulation of different size of audio file performance on different algorithm

Audio File	File 1	File 2	File 3	File 4	File 5	File 6	Average Time
Audio Size(KB)	3453	3823	4012	4434	4990	6734	5336.72
Two fish	142	163	171	194	410	431	296.06
AES	160	176	195	221	467	497	336.31
Blowfish	151	171	172	212	443	487	321.67

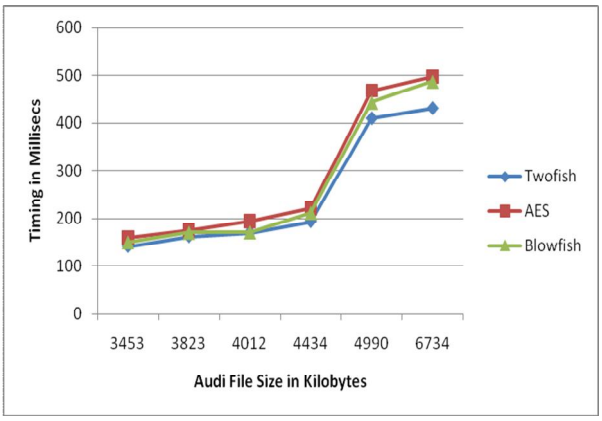

Figure 7: Performance graph for Audio files

4. CONCLUSION

From the above experiments, we come to know that the algorithm works differently for different input files but not based on the capacity or memory size of the input files. It is useful to select the correct algorithm for exact input files to share between the two nodes within time. In future, we can similarly do these types of testing on different system configuration and algorithm with different inputs.

REFERENCES

1. Prerna Mahajan and Abhishek Sachdeva. **A Study of Encryption Algorithms AES, DES and RSA for Security**, *Global Journal of Computer Science and Technology Network, Web & Security***,** vol. 13, no. 15, pp. 15-22, Jan.2013.
2. Carlos Rompante Cunha, Elisabete Paulo Morais, João Paulo Sousa, and João Pedro Gomes. **The Role of Cloud Computing in the Development of Information Systems for SMEs**, *Journal of Cloud Computing*, vol.2017, pp.1-7, Feb.2017. https://doi.org/10.5171/2017.736545
3. S.Hirani. **Energy Consumption of Encryption Schemes in Wireless Devices**, University of Pittsburgh, 2008.
4. P.Ruangchaijatupon, and P.Krishnamurthy. **Encryption and power consumption in wireless LANs- N**, *Telecommunication Program*, pp. 148-152, Jan. 2001.
5. Aamer Nadeem, and M.Younus Javed. **A Performance Comparison of Data Encryption Algorithms**, , in *Proc. International Conference on Information and Communication Technologies*, IEEE, 2005, pp.84-89.
6. S. Z. S.Idrus, and S. A. Aljunid. **Performance analysis of encryption algorithms text length size on web browsers**, *IJCSNS International Journal of Computer Science and Network Security*, vol. 8, no. 1, pp. 20-25, Dec. 2008.
7. Avinash Ghorpade, and Harshavardhan Talwar. **The Blowfish Algorithm Simplified**, *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 5, no. 4, pp. 3343-3351, Oct. 2016.
8. Bulusu Rama, K. Sai Prasad, and P.Sreeja. **Secure k-NN query on encrypted cloud data with multiple keys**, vol. 8, no. 3, pp.874-878, May 2019. https://doi.org/10.30534/ijatcse/2019/82832019
9. M.RobinsonJoel, M.Navaneethakrishnan, T.D.Jeba Freeda and R. Arunadevi. **An Analysis On Storage And Security Over Cloud Platform**, *The International Journal of analytical and experimental modal analysis*, vol. 12, no. 1, pp. 2222-2226, Jan.2020.
10. G.N.Krishnamoorthy, D.V. Ramaswamy, and M.G.Leela. **Performance Enhancement Of Blowfish Algorithm By Modifying Its function**, *Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications*, pp. 241-244, July 2007. https://doi.org/10.1007/978-1-4020-6266-7_44
11. Bruce Schneier. **Description of a new variable-length key, 64-bit block cipher (Blowfish) Fast Software Encryption**, Lecture notes on Computer Science, 1993, pp. 191-204. https://doi.org/10.1007/3-540-58108-1_24
12. Anjana Devi, and B. S. Ramya. **Two fish Algorithm Implementation for lab to provide data security with predictive analysis**, *International Research Journal of Engineering and Technology*, vol. 4, no. 5, pp.3033-3036, Jan. 2017.
13. Much Aziz Muslim, Budi Prasetiyo, and Alamsyah. **Implementation Twofish Algorithm For Data Security In A Communication Network Using Library Chilkat Encryption ActiveX**, *Journal of Theoretical and Applied Information Technology*, vol. 84, no. 3, pp.2005-2016, Feb.2016.
14. Rizky Riyaldhia, Rojalia, and Aditya Kurniawanb. **Improvement Of Advanced Encryption Standard Algorithm With Shift Row And S.Box Modification Mapping In Mix Column**, in *Proc. 4th International*

Conference on Computer Science and Computational Intelligence, Indonesia, 2017, pp.401-407.

15. David Smekal, Jakub Frolka, and Jan Hajny. **Acceleration of AES Encryption Algorithm Using Field Programmable Gate Arrays,** *International Federation of Automatic Control*, vol.51, no.6, Jan. 2016. https://doi.org/10.1016/j.ifacol.2016.12.075
16. J.Probell. **Architecture considerations for multi-format programmable video processors**, *Journal of signal processing systems*, vol.50, no.1, pp. 33-39, July 2007.
17. S.Wong, S.Vassiliadis, and S.D.Cotofana. **Future directions of (programmable and reconfigurable) embedded processor,** *domain-Specific Processors: Systems, Architectures, Modeling, and Simulation*, vol.1, no. 27, pp. 235-257, 2004.
18. V.Sakthivelmurugan, R.Vimala, and Aravind Britto. **Star hotel hospitality load balancing technique in cloud computing environment**, *Advances in Intelligent Systems and Computing***,** vol. 750, pp.119-126, March 2019.
19. V.Sakthivelmurugan, R.Vimala, and Aravind Britto. **Magnum opus of an efficient hospitality technique for load balancing in cloud environment**, *Concurrency and Computation: Practice and Experience*, vol. 31, no. 14, pp. 1-11, Nov.2018. https://doi.org/10.1002/cpe.5078
20. M.Robinson Joel, V.Ebenezer N.Karthik, and K.Rajkumar. **Advance dynamic network system of internet of things**, *International Journal of Recent Technology and Engineering*, vol. 8, no. 3, pp.6209-6212, Sep.2019. https://doi.org/10.35940/ijrte.C5657.098319
21. V.Sakthivelmurugan, R.Vimala, and K.Rajkumar. **Thershold Max Method for Load Balancing in Cloud Computing**, *Asian Journal of Research in Social Sciences and Humanities*, vol. 7, no. 2, pp.640-650, Nov. 2017. https://doi.org/10.5958/2249-7315.2017.00117.4
22. V.Sakthivelmurugan, and K. Rajkumar. **SAKTHI: Scheduling Algorithm K to Hybrid in Cloud Computing** , *International Journal for Research in Applied Science & Engineering Technology*, vol. 3, no. 5, pp.124-127, May 2015.
23. Adel Abdullah Abbas. **Cloud-based Framework for Issuing and Verifying Academic Certificates**, *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 6, pp.2743-2749, Nov.2019. https://doi.org/10.30534/ijatcse/2019/10862019
24. Abdallah Ghourabi, and Mohamed Jelidi. **Experimental Evaluation of a Hybrid Intrusion Detection System for Cloud Computing**, *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 6, pp.3065-3073, Nov.2019. https://doi.org/10.30534/ijatcse/2019/65862019