Available online at www.worldscientificnews.com

World Scientific News

An International Scientific Journal

WSN 112 (2018) 244-251 EISSN 2392-2192

SHORT COMMUNICATION

Performance of Symmetric Key Cryptography Algorithms in Cloud Storage

Hind Osman, Sara M. Ibrahim, Elmustafa Sayed Ali*

Department of Electrical and Electronics Engineering Faculty of Engineering, Red Sea University,
Port Sudan, Sudan

*E-mail address: elmustafasayed@rsu.edu.sd

ABSTRACT

Today cloud computing becomes one of the most attractive topics due to the wide opportunities that is provided which aims to enhance the electronic services to a higher-level providing cost saving, expanding possibilities, storage in demand and the huge intake capability as well. Security is one of the most important process that should be implemented in every cloud structure level, especially with data in case of processing or storing to keep it save from unauthorized access to overcome the security challenges and difficulties, which face both provider and users in cloud. In this paper a study to compare the security algorithms for encryption/decryption files has been done to evaluate the performance impact with memory capacity, processing time and algorithms running time. The comparison has been done between three encryption algorithms AES, DES, and Blowfish to determine the performance of each one in cloud storage. From the experimental results we found that DES is faster in running time compared to other algorithms as well as AES considered to be the safest one in data protection.

***Keywords*:** Cloud Computing, NetBeans, Google Drive Storage, AES, DES, BLOWFISH

(Received 12 October 2018; Accepted 22 October 2018; Date of Publication 23 October 2018)

1. INTRODUCTION

Many security issues are used for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. Data protection law requires data controllers to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or loss unauthorized alteration, disclosure or access in particular where the processing involves the transmission of data over a network [1].

When applying the data security requirement to cloud computing, a number of points should consider in protecting data, including the fact that use of a cloud vendor increases the potential for unauthorized disclosure or access. Accordingly, authentication and access safeguards must be robust and provide for an appropriate level of security. Due to the increased level of public access to the cloud, the risk of an information security breach is correspondingly higher, thus the cloud provider should be required by contract to inform data controllers of any data breach incidents [2].

2. CLOUD STORAGE

Cloud data storage consists of a huge number of storage devices that distributed throughout the network; it also provides users with the normal structure of the cloud data storage, which include distributed file system, resource pool, service interfaces and service level agreements. The definition of cloud storage is a branch of Cloud Infrastructure as a Service (IaaS) in cloud computing and it is working to provide the data, and reduce infrastructure costs by storing data remotely [3]. Cloud data storage works to provide storage service for different levels of customers as the cost of storage depends on the space required the ability and bandwidth. Cloud storage can be divided into two parts; cloud storage that is designed using encryption technologies and has no theoretical framework for encryption and Cloud storage that is using encryption techniques and it has theoretical framework for encryption [4].

3. CRYPTOGRAPHIC ALGORITHMS

Many types of cryptographic algorithms have been designed for data security issues security and categorized depending on the process of encryption key. The most well-known algorithms those used with data security are briefly discussed in the following sections.

A. DES Algorithm

The DES algorithms are block Cipher which is designed to encrypt and decrypt blocks of data consisting of 64 bits by using a 64-bit key. The algorithm goes through 16 iterations that interlace blocks of plaintext with values obtained from the key. The algorithm transforms 64-bit input in a series of steps into a 64bit output. The same steps, with the same key are used for decryption. DES is still widely used by financial services and other industries worldwide to protect sensitive on-line applications [5].

B. Blowfish Algorithm

Blowfish algorithm is a symmetric block cipher which can be used as a drop-in replacement for DES. It takes a changeable length key, from 32 bits to 448 bits, which makes it perfect for both exportable and domestic use. Blowfish was designed as a free alternative to the present encryption algorithms. All operations in blowfish are additions on 32-bit words and XOR. Blowfish is a fast algorithm can encrypt data on 32-bit microprocessors and it is a symmetric block encryption algorithm designed in consideration with fast run time, low memory usage and simple process with promising secure procedure [6].

C. AES Algorithm

AES is based on rijndael algorithm which is a symmetric block cipher that processes fixed data of 128-bit blocks. It supports key sizes of 128, 192 and 256 bits and consists of 10, 12 or 14 iteration rounds, respectively. This standard may be used by Federal departments and agencies when an agency determines that sensitive (unclassified) information requires cryptographic protection [7]. The algorithm specified in this standard may be implemented in software, firmware, hardware, or any combination thereof. The specific implementation may depend on several factors such as the application, the environment, and the technology used.

4. SIMULATION MODEL

In this paper we evaluate the performance of three algorithms used for encryption and decryption they are; DES, Blowfish and AES to secure different sizes of files 5kb, 10kb, 15kb, 20kb and 25 kb by using NetBeans to write the algorithms as a Java script then connecting the NetBeans platform with Google drive to provide cloud space for files storage. In NetBeans platform the java codes for each algorithm entered using computer with certain specifications: Processor Intel (R) Celeron (R) CPU 2.20 GHZ, Installed memory (RAM) 2.00 GB, and in operating system Windows 7. The simulation parameters are shown in the Table 1 below.

Table 1. Simulation Parameters.

Parameters	Type
Algorithms	AES, DES and BLOWFISH
Cloud Type	Cloud storage
Cloud Storage	Google drive
Processor	Intel (R) Celeron 2.20 GHZ
Memory Usage (RAM)	2.00 GB
Algorithms Platform	Net beans

File size	5, 10, 15, 20 and 25 kb
Key Size	128, 32 to 448 and 56 bits

5. SIMULATION RESULTS AND DISCUSSION

After implementing the algorithms in NetBeans with google drive, we calculated the performance metrics as follows; the *Rum Time* is difference between starting and ending time of encryption taken by particular algorithm. *Memory Space* by the system and the *CPU Time* which defines the processing time to impalements each algorithm. The result we obtained are discussed in two scenarios; scenario 1 reviews the results of the algorithms performance in local storage. And scenario two discuss the results of the performance in cloud storage.

A. Scenario 1: Security Algorithms Performance in Local Storage

In This scenario, the figures below present the performance of AES, DES and blowfish algorithms with different file sizes stored in local storage.

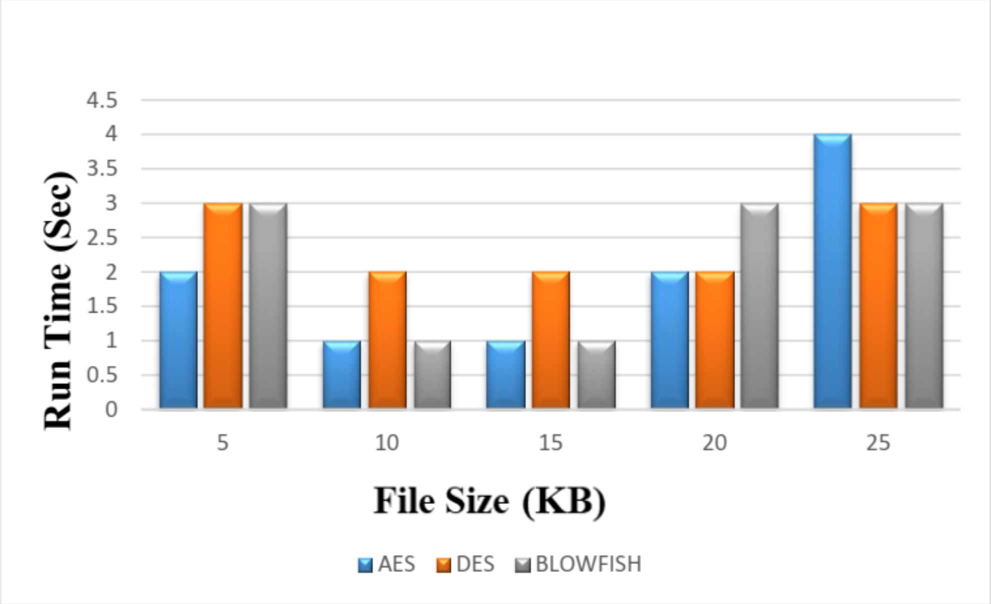

Figure 1. Run Time performance of security algorithms in local storage

From Figures above, we observed that AES has highest run time with large file size and lowest run time in case of small file sizes compared to other algorithms DES and Blowfish as shown in Figure 1. The reason because that AES has a large block size and it sometimes causes encrypted messages to be slightly longer which will lead to increase the setup and processing time even it has a quick key setup but with small file sizes.

In Figure 2 DES remains to be executed with low CPU time and Blowfish took more time with CPU utilization to complete the process specialty with large file sizes. Since the files size are within a range of Kb all algorithms use a small local memory size for encryption and decryption processes as observed in Figure 3 above. Finally, we observed that DES is suitable with large file sizes which will take short CPU time to be executed and lower run time when compared to others.

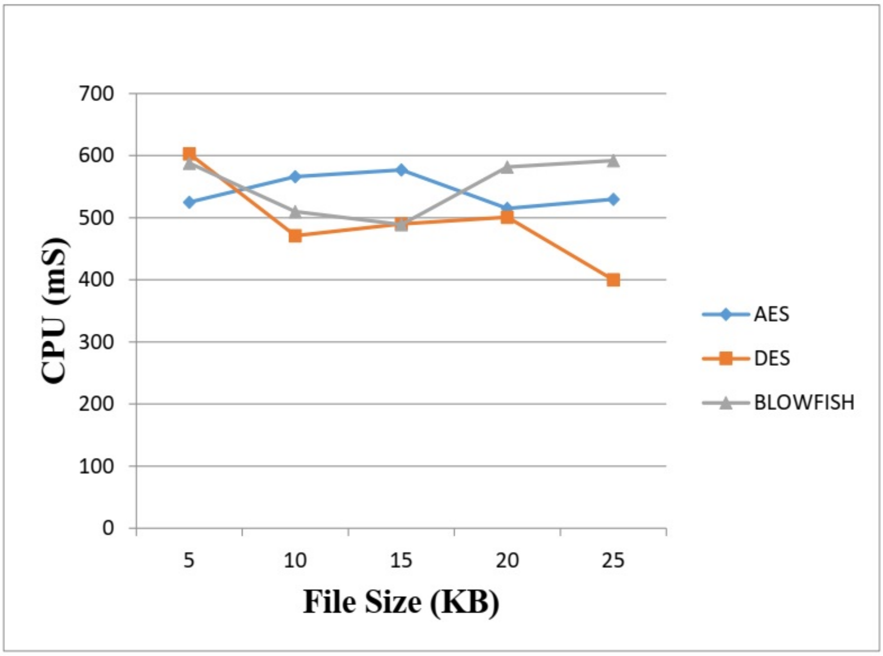

Figure 2. CPU performance of security algorithms in local storage

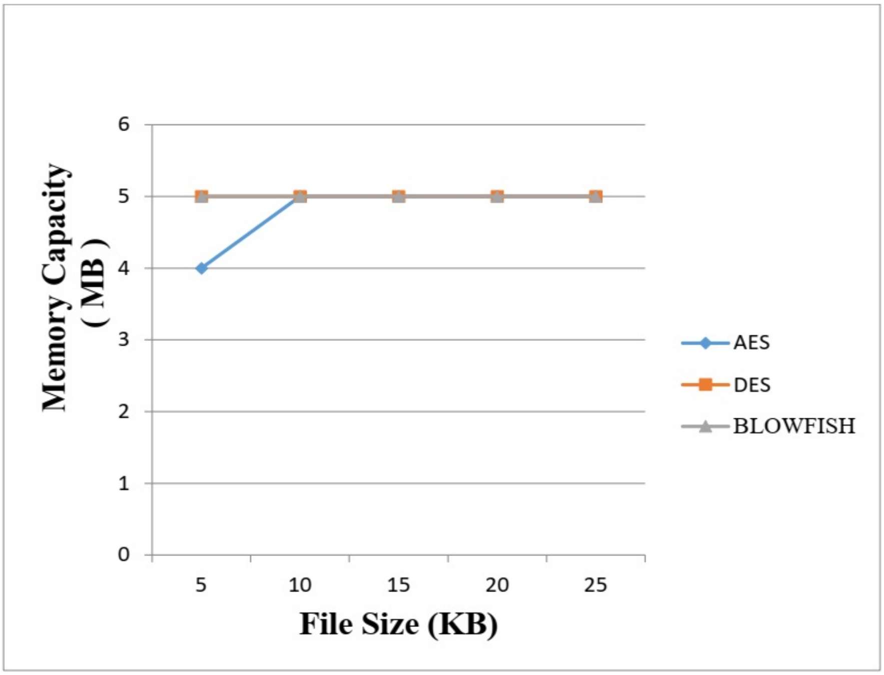

Figure 3. Memory Load performance of security algorithms in local storage.

B. Scenario 2: Security Algorithms Performance in Cloud Storage

This scenario, reviews the performance of AES, DES and blowfish algorithms in cloud storage and obtained their impact on processing time, and memory usage as shown in the following figures below.

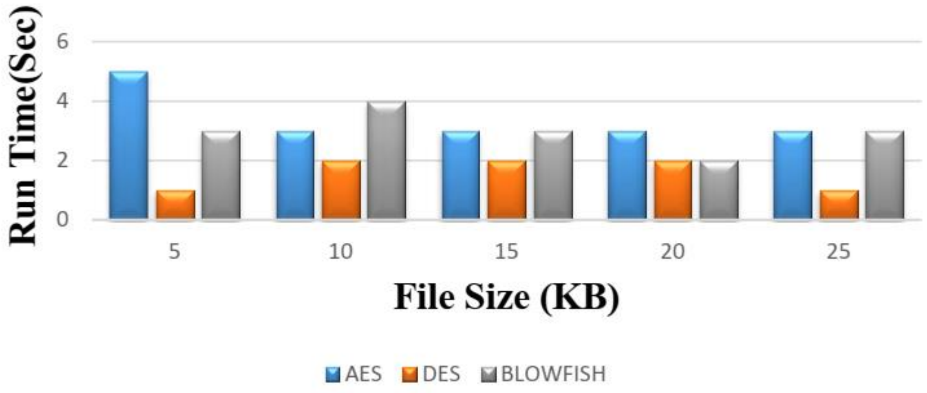

Figure 4. Run time performance of security algorithms in cloud storage

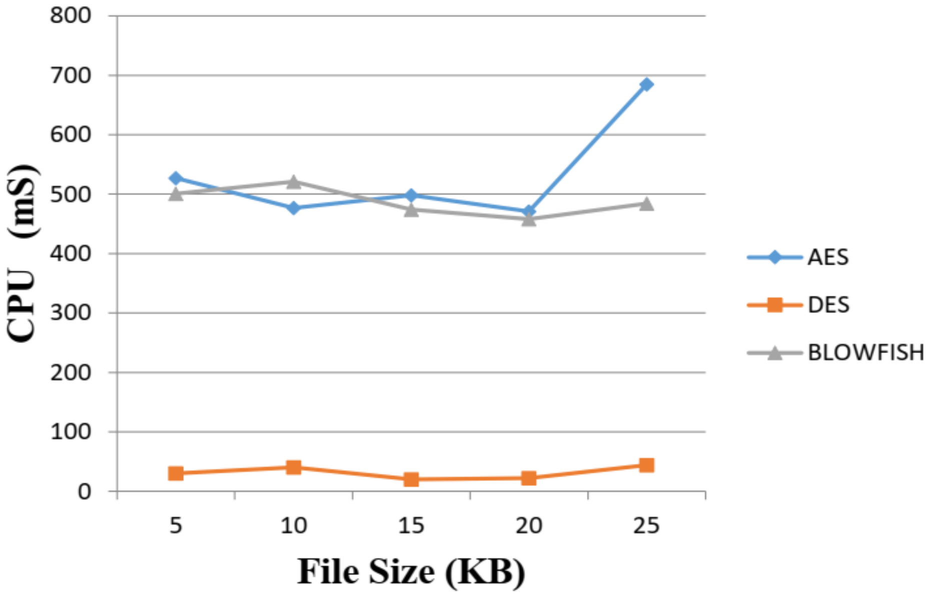

Figure 5. CPU performance of security algorithms in cloud storage

From Figures 4, 5 and 6 above we notice that AES algorithm with all files size, has greater amount of time because key generation time. The results of run time and CPU time has higher value compared to the other algorithms specially in CPU time with large file size this happen because of large time taken for key recovery time from server which depends on cloud access control polices. DES exhibited lesser amount of time for all in execution and CPU compared to the other algorithms. Although in some instances Blowfish got better results in CPU time. With regards to decryption/encryption time, the result of the experiment and it is obvious by looking at the figures above that as the data load becomes bigger, the lesser the time spent by DES over the other two algorithms, that means DES is highest speedup in comparison to others. As observed in overall scenarios the cloud memory capacity is reduced compared to local storage while also DES algorithm in cloud takes low values for running time, memory capacity and less CPU time compared to other algorithms such as Blowfish & AES.

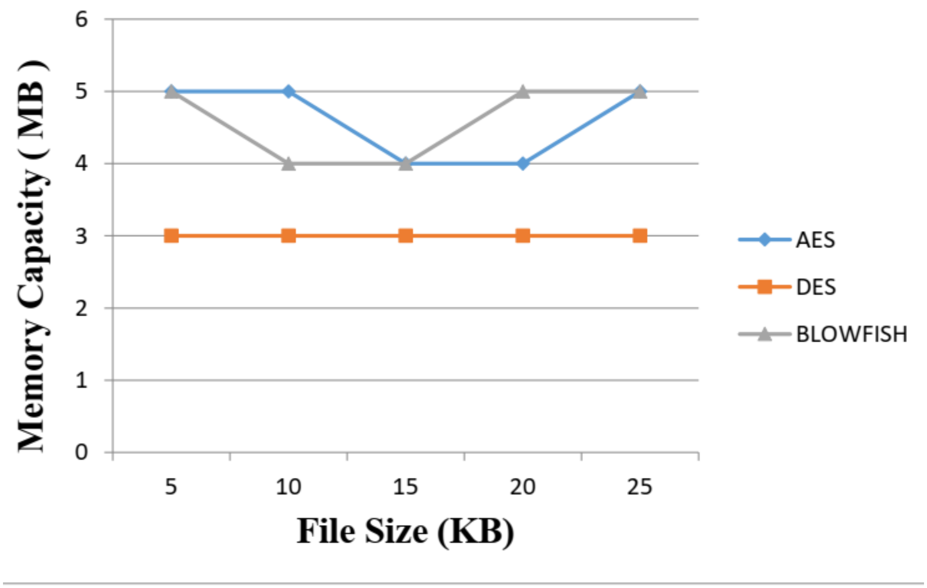

Figure 6. Memory load performance of security algorithms in cloud storage

6. CONCLUSION

As known that in generally, the storage of data occurs in servers, therefore as a result of rapid increasing of data thus require more additional servers to be installed. These servers take both wide areas & positions lead to more cost. Cloud storage considered to be a final solution to such a problem. It's defined as virtual servers carry a large quantity of data. The comparison has been done between three encryption algorithms to determine the performance of each one in cloud storage and the result showed that DES is faster in running time compared to other algorithms as well as AES considered to be the safest one in data protection.

Authors

Hind Osman She is presently doing B.Sc. degree with honors in red sea university faculty of Engineering, complete her graduate research in September 2018. Her research interest on field MANETs and Wireless Networks.

Sara M. Ibrahim She is presently doing B.Sc. degree with honors in red sea university faculty of Engineering, complete her graduate research in September 2018. Her research interest on field MANETs and Wireless Networks

Elmustafa Sayed Ali received his M.Sc. degree in electronic engineering, Telecommunication in 2012, and B.Sc. (Honor) degree in electrical engineering, Telecommunication in 2008. He was a wireless network (Tetra system, Wi-Fi and Wi-Max) engineer in Sudan Sea Port Corporation for 5 years and a head department of electrical and electronics engineering, faculty of engineering in Red Sea University for one year. He published papers on wireless communications and networking in peer-reviewed academic international journals and book chapters in big data clouds. His areas of research interest include MANETs, wireless networks, VANETs, image processing, computer networks, and Cloud computing.

Reference

[1] R. Saranya, V.P. Muthu Kumar, Security issues associated with big data in cloud computing, *International Journal of Multidisciplinary Research and Development* Volume 2, Issue 4, 580-585, April 2015.

[2] Lisa J. Sotto, Bridget C. Treacy, and Melinda L. McLellan, Privacy and Data Security Risks in Cloud Computing, Reproduced with permission from Electronic Commerce & Law Report, Copyright 2010 by The Bureau of National Affairs, Inc. (800372-1033).

[3] Ahmed Shawish and Maria Salama, Cloud Computing: Paradigms and Technologies, *Techniques and Applications, Studies in Computational Intelligence* 495, DOI: 10.1007/978-3-642-35016-0_2 Springer-Verlag Berlin Heidelberg 2014.

[4] Hamdan M. Al-Sabri, Saleh M. Al-Saleem, Building a Cloud Storage Encryption (CSE) Architecture for Enhancing Cloud Security. *International Journal of Computer Science* Issues, Vol. 10, Issue 2, No 1, March 2013.

[5] Gurpreet Singh, Supriya Kinger. Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security. *International Journal of Scientific & Engineering Research,* Volume 4, Issue 7, July 2013.

[6] Gurjeevan Singh, Ashwani Kumar, K. S. Sandha. A Study of New Trends in Blowfish Algorithm. *International Journal of Engineering Research and Applications* 2014, Vol. 1, Issue 2, pp. 321-326.

[7] Prachi V. Bhalerao1 et al. Hardware Implementation of Cryptosystem by AES Algorithm Using FPGA. *International Journal of Computer Science and Mobile Computing,* Vol. 6 Issue 5, May 2017, pg. 84-89.