DEVELOPMENT OF BLOWFISH ENCRYPTION SCHEME FOR SECURE DATA STORAGE IN PUBLIC AND COMMERCIAL CLOUD COMPUTING ENVIRONMENT

By

SHAFI'I MUHAMMAD ABDULHAMID * NAFISAT ABUBAKAR SADIQ ** MOHAMMED ABDULLAHI ***
NADIM RANA **** HARUNA CHIROMA ***** DADA EMMANUEL GBENGA ******

** Department of Cyber Security Science, Federal University of Technology Minna, Nigeria.*
*** Department of Computer Science, Ahmadu Bello University Zaria-Nigeria.*
**** College of Computer Science and Information Systems, Jazan University, Jazan, Kingdom of Saudi Arabia.*
***** Department of Computer Science, Federal College of Education (Technical), Gombe, Nigeria.*
****** Department of Computer Engineering, University of Maiduguri, Maiduguri, Nigeria.*

Date Received: .../.../..... *Date Revised: .../.../.....* *Date Accepted: .../.../.....*

ABSTRACT

Cloud computing is defined as the delivery of on- demand computing resources ranging from infrastructure, application to datacenter over the internet on a pay-per-use basis. Most cloud computing applications does not guarantee high level of security such as privacy, confidentiality and integrity of data because of third-party transition. This brings the development of Blowfish cloud encryption system that enables them to encrypt their data before storage in the cloud. Blowfish encryption scheme is a symmetric block cipher used to encrypt and decrypt data. Microsoft Azure cloud server was used to test the proposed encryption system. Users are able to encrypt their data and obtain a unique identification to help them retrieve encrypted data from the cloud storage facility as when needed.

Keywords: Blowfish Encryption, Cryptography, Cloud Computing, Data Storage, Encryption Scheme.

INTRODUCTION

Clouds computing generally refer to data being stored centrally in cloud and are accessible to clients through thin clients and lightweight mobile devices. Cloud computing infrastructures over time have provided a way for data to be stored and accessed by customers easily giving the availability of internet connection. Cloud computing maintenance and technical services are provided by cloud provider who must ensure the quality of services. Cloud computing has offered better storage facilities to schools, organizations, financial institutions, traders and government offices. Data stored in cloud computing applications serves as backup in case of loss of data in an unlikely event (Latiff, Abdul-Salaam, & Madni, 2016, Xia, Wang, Sun, & Wang, 2016; Rittinghouse, & Ransome, 2016).

Cybercrimes or internet crimes are unlawful action carried out using the internet or cyber environment by loopholes, weaknesses and vulnerability of a system Internet Crime Complaint Center (IC3). The need for information security increases as technology advances which also allows for free information obtaining tools online such as whois lookup. Data retention therefore needs a more secured platform for storage of data. Note that the accessibility and availability of this data to potential authorized users must be made easy. Data owners are motivated to outsource their complex data management from local sites to commercial public cloud for great flexibility and economic savings brings about the advent of cloud computing which has by far provide the best platform for authorized users.

Encryption is used to convert data in to a form that is not comprehensive to unauthorized users with unauthorized access to data stored or on transit. Encryption is a method used in ensuring privacy, confidentiality, integrity and authenticity of data (Abdullahi, & Ngadi, 2016; Said, 2005) Over time encryption have been used to hide or protect information of high secrecy and since the advent

of cloud computing which provides a pay-per-use platform to outsource our data. Human have referred back to the way of hiding data back in 1500BC which is now known as encryption. Encryption or the ability to store and transmit information in a form that is unreadable to anyone other than the intended person, it's a critical element of our defense to these attacks. (Kaur,& Singh, 2013).

Blowfish encryption scheme is a symmetric block cipher designed by Bruce Schneier in 1993. It includes a huge number of encryption product and was designed as an alternative to replace the obsolete Data Encryption Scheme (DES). Blowfish takes a variable length of 32bit to 448bit with a default of 128bit. Blowfish is unpatented and license- free which allows for its free availability to users (Schneier, Schneier on Security). Blowfish is fit for applications whose key does not change often for instance an automatic file encryptor or a communication link (check for more instances). It is relatively faster than DES when implemented on a 32-bit microprocessor with huge caches such as Pentium and PowerPC. The blowfish algorithm consists of two parts; a key-expansion and a data-encryption part. The key-expansion part refers to the conversion of a key into many sub-keys. Data encryption occurs through a 16-Feistel Network. Each round consists of a key dependent permutation, a key and data dependent permutation (Xia, Wang, Sun, & Wang, 2016; Krishnamurthy, Ramaswamy, Leela. & Ashalatha, 2008).

The main contributions of this research manuscript are chronicled as follows:

- We put forward a symmetric block cipher called blowfish encryption scheme for secure data storage in public and commercial cloud computing environment.
- We developed an application for protection of third-party data using the proposed scheme above in infrastructure as a servicecloud.
- We tested and evaluated the developed encryption application with standard metrics and compares with previous related encryption schemes.

The aim of this research paper is to developed Blowfish encryption scheme for secured data storage in public and commercial cloud computing environment. The remaining parts of the paper is organised as follows: Section II, presents the problem statement. Section III details the analysis of previous related literatures. Section IV, details the research methodology whereas Section V, presents the Blowfish encryption scheme. In Section VI, we present the implementation procedure. Then the performance evaluation was done in Section VII. Conclusion and recommendations were presented in Section VIII.

1. Problem Statement

Cloud computing applications are designed for clients to outsource their data, access their outsourced data over the internet and also serve as backup for individuals ranging to organizations, schools and financial systems. Cloud applications which includes Cloud App, Waze, Box.net, AudioBox.fm, Jouku, icloud does not ensure absolute security in terms of privacy, integrity and confidentiality of the data, because of third-party intervention. This brings about the development of blowfish encryption scheme application to properly secure user's data in both public and commercial.

2. Literature Review

Thakur and Kumar (2011) conducted simulation of commonly used symmetric encryption scheme which involves Data Encryption scheme (DES), Advanced Encryption Scheme (AES) and Blowfish algorithm. The simulation was put into practice using Java programming language and the types of encryption/decryption mode. The encryption/decryption mode is Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher feedback (CFB) and Output Feedback (OFB). EBC; data is divided into 64- bit block with each block been divided are encrypted once at a time. CBC involves an already encrypted block to be XORed with the next plaintext making each block dependent on previous blocks. CFB mode enables encryptor to handle plaintext that is not up to 64-bit by adding dummy byte to enable encryption of the plaintext. OFB is same as CFB but less secure than CFB

because it requires the only the real ciphertext to find the previous plaintext. Java Cryptography Extension (JCE) and Java Cryptography Architecture(JCA) containjava.cypto and java.security that manages wrappers for DES, AES and Blowfish. The algorithm setting shows that the plaintext is divided in small block size (bits) and key size (bits). The simulation was conducted more than once to achieve accurate result necessary for comparing the different algorithm, and the AMDS empron processor with 2GB RAM was used. Compilation of the simulation program was made possible with the use of 1.7 development kit for java in its default settings. Result of these comparison with different data load and the mode of encryption/decryption shows that blowfish has better performance than AES and DES interms of processing time.

Chaplot, (2015) used MATLAB to design and implement blowfish in Matlab for encrypting and decrypting images. The paper includes the description of blowfish algorithm as involving a 16 round feistal network for encrypting data. A feistal network refers to means of changing functions to permutation. Akshit et al. further gave steps of how the feistal network works. The fiestal network first split a block of divided message into two equals. It then swaps the halves of the divided message. A function and a key applied to the other halve and then XORed. It further shows that Blowfish algorithm consists of two parts; data encryption and key expansion parts. The advantages of blowfish stated here includes; been accepted as one of the strongest technique, unpatented and license free, highest speed algorithm known. The disadvantages include being vulnerable to attacks on weak keys, cannot be used for files more than 4GB because of its small bit block size and blow fish has successors. The simulation shows how blowfish can be implemented on a different platform (MATLAB) and used to conceal animage.

Gahi, Guennoun, and khatib (2000) listed a few security issues that the cloud service encompasses and possible solution to the listed problems. In a case of loss of physical security, secure data transfer was proposed. To ensure data integrity during transfer, storage and retrieval, a secure software interface is a possible solution. Data separation ensures the privacy of data from being shared to other parties. NetBeans IDE with Java was used to implement AES, DES, RSA and blowfish algorithms. The implementation of multiple algorithms gives users an opportunity to use the security algorithm of their preference. Comparison of the algorithm was further carried out interms of platform, keysize, keyused, scalability, initial vector size, security, data encryption capacity, authentication type. Memory usage and execution time. Different parameter used for comparison for the different encryption scheme so far shows that AES execute in less time, Blowfish memory requirement is as low as 5kb, more encryption time is being used by DES and RSA use the longest memory size and execution time.

Curino et al., (2011) introduced a hybrid technique of security algorithm, a combination if RSA and BLOWFISH. The consideration of such combination was based on the fact that blowfish is effective and unpatented which makes the cryptosystem cost effective and RSA which is almostalways considered for its digital signature. The proposed technique can be used for cloud computing on FPGAnetwork.

Symmetric and asymmetric features of the chosen algorithm allow the use of small keysize forth easymmetric technique. The symmetric technique always uses high key size to reduce the possibility of direct key substitution. The hybrid technique can be applied to the third layer of cloud computing. FPGA is easily used to implement the hybrid technique and it uses little resources out of the available resource. Analysis of the implementation response on FPGA shows that the combination of the two algorithms is better than any other technique. The proposed technique is further implemented using VHDL, hence, the algorithm is secured and ensures better authentication for cloud computing data.

Itani, Kayssi, Chehab, (2009) presented 'A performance based comparison of various symmetric cryptographic algorithms in runtime scenario'. The purpose of the paper is based on the detail analysis of the terms, concepts, terminology and analysis of some of the cryptographic schemes (AES, DES and BLOWFISH). Authentication, privacy, integrity and non-repudiation were mentioned as

the security requirement need for a secured communication. Cryptography is of 3 types which are; symmetric or secret key cryptography, asymmetric or public key cryptography and hash function. The secret key cryptography is of two classifications; stream cipher and block cipher. Encryption and decryption has models of operation namely; Electronic code book (ECB), Cipher blocks chaining (CBC), Cipher feedback (CFB) and output feedback (OFB). A detailed analysis of the few symmetric encryptions was given and also the performance result of the symmetric encryption scheme in the different model of encryption and decryption were given. It was deduced that asymmetric algorithm consume more time than symmetric algorithm.

Li, Yu, Cao, and Lou, (2011) proposed Effective Privacy Protection scheme (EPPS) to satisfy users privacy and also ensure performance of cloud systems in different environment. Cloud data protection system (CDPS) which includes detailed EPPS and description of its content. Chuang et al gave a detailed description of the CDPS architectural components which are quantification models, privacy analysis, data protection procedure and data division. Simulation environment used are; PC with intel core 2 Duo E8400 3.0GHz CPU and a CentOS 5.2 operating system. The result of the simulation shows that the scheme's total cost time more than the other algorithms the scheme isbeing compared with. The security of the scheme is also found out to be effective despite a 46% subtraction to be able to compare it with other security algorithm. The scheme is said to be an effective means of protecting users' privacy and performance in the cloud environment with increasing the performance overhead of the system.

Schneier (n.d) proposed the use of different encryption algorithms to increase privacy of data in the cloud. Thecloud types and characteristics were discussed to give an understanding of what the cloud entails and its services that benefit owners of data. In a given analysis between RSA, DES, AES and BLOWFISH it was discovered that Blowfish key length is larger than that of AES. The is implemented using JDK 1.6 Eclipse IDE. Google app Engine SDK 1.6.0. The scheme allows a user to select and encryption scheme of their choice after authenticating into the cipher cloud. The data of preference is then sent to the cloud server, the sever then decrypt the request with a generated symmetric key and further encrypt it with RSA.

Hashem et al (2015) proposed a cloud based architecture for owners of data to ensure confidentiality and privacy of their data. The architecture provides a user friendly framework that enables the selection of an encryption algorithm. The framework includes steps every user pass through to secure their data. A user will require a form of authentication which requires Id and password. After a successful authentication, the user is presented with a list of options (view files, upload files, delete files and download files). Theuploadfilesbutton will transmit the user's data to the cipher cloud through an encrypted connection using HTTPS and the file is encrypted using a symmetric scheme chosen by the user. Downloading of a selected file by the user will be decrypted with the previous selected scheme. A new user will be required to create an account using google account and other steps to successfully upload a file are displayed for the user.

Lee, Chung, and Hwang, (2013) presented a detailed analysis of commonly used symmetric encryption system (AES, DES, 3DES and BLOWFISH) and asymmetric encryption system (RSA). Symmetric scheme was found out to be faster than asymmetric key encryption. The analysis includes a table that shows the difference and similarities between the symmetric algorithms which indicate the superiority of blowfish as compared to another encryption algorithm.

3. Materials and Method

The research work is based on converting data into a non-comprehensible form using Blowfish encryption scheme. The scheme is a symmetric algorithm, which means that it requires same key for encrypting and decrypting messages. Individuals who intend to save their data in the cloud can adopt this method to convert data of their choice before outsourcing it to commercial cloud as shown in Figure 1.

Cloud user (send/retrieve) is the owner of the data that is supposed to be sent to the cloud environment. The

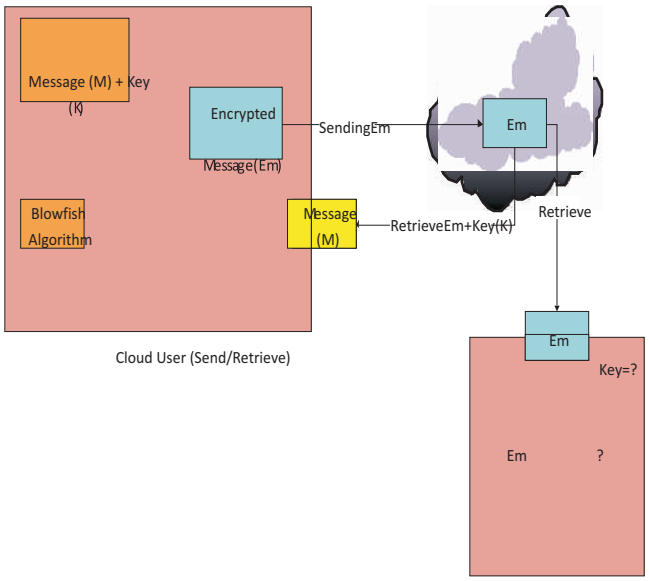


Figure 1. Conceptual Framework of the Cloud Encryption System

clouduser has a message (M) which he or she wishes to encrypt. Akey (K) is needed for encrypting the message. Blowfish is the algorithm used for the encryption and decryption process. Encrypted message (Em) is then send to the cloud via a secure communication protocol HTTPS. The cloud service knows the message to be Em which is not comprehensible to an attacker given the possibility that the cloud system is compromised. Em would be retrieved but the key remains unknown to the attacker. These gives an owner of data stored in the cloud an edge or another level of security over other owners using same cloud system.

Where

$k \in K$ is a secret key from a set of keys in K

$m \in M$ is a set of possible embedded messages in M

$c \in C$ is a set of audio containers in C

$s \in$

S is a set of stegos generated by embedding m in c

$\therefore$

audiosteganographic system for information hiding can be divided into two stages:

an embedding transformation stage and extraction of information stage.

Let embedding tranformation be represented as $E_m T$

Extraction tranformation be represented as $E_x T$

$\therefore$

$E_m T : C \times K \times M \rightarrow C$

$E_x T : C \times K \rightarrow M$

Such that

for $m \in M$, $c \in C$ and $k \in K$

$$m = E_x T(E_m T(c, k, m), K) \quad (1)$$

$$s = E(c, k, m) \quad (2)$$

let P_c represent the distribution of probabilities of steganographic containers c or $P_c(C)$

P_s represent the distribution of probabilities of embedded stego - object s or $P_s(S)$

Using relative entropy, it shows that the distribution (D) of P_c and P_s are compared

$$(P\ P) = \sum_{c,s} \quad \sum_{c \in C\ c} P(C) \log \frac{P_c(c)}{P_s(S)} \quad (3)$$

Interpretation of model expressed in equation (3)

$$(a) \quad If\ P_c(C) = P_s(S) \Rightarrow$$
$$(P_c, P_s) = \sum_{c \in C} P_c(C) \log(1) \qquad where \log(1) = 0$$
$$(P_c, P_s) = 0 \quad (4)$$

This shows that the stegosystem is absolutely secured. The attacker cannot differentiate between the stego-audio and the container

(b) $(P_c, P_s) \leq \varepsilon$ where ε is a non-negativevalue implies that the stegosystem is ε -secured. The smaller the value of ε, the more secure the stegosystem.

4. Blowfish Encryption Scheme

The flowchart diagram analyses problems in other to achieve a possible solution as shown in Figure 2.

In Figure 2, x is a 64-bit plaintext to be encrypted, dummies are added to a plain text that is not up to 64-bit. X is divided into two equal halves, that is 32-bit; leftmost plaintext (xL) and rightmost plaintext (xR).

p is an array of 18, 32-bit subkey, which is XORed with the leftmost 32-bit of plaintext and the result is passed to the f function of blowfish.

The result becomes the rightmost 32-bit for the next round, and the output of F function is XORed with the original rightmost 32-bit of plaintext, becomes leftmost 32- bit and

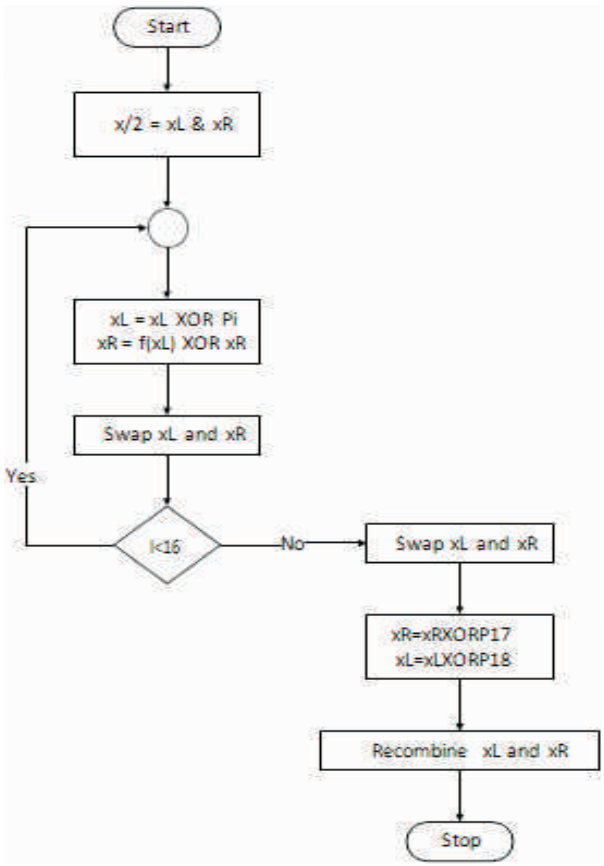


Figure 2. Blowfish Encryption Flowchart

so on as shown in Figure 3.

The database design which was done in Microsoft Azure's cloud platform consists of a table with four fields which are ID, unique ID, username and ciphertext. This allows user information to be stored and retrieved when needed.

5. Implementation

The software is developed using C#, Visual Studio and Microsoft Azure platform due to the characteristics they possess and how they are closely associated. C#is referred to as a modern, object-oriented programming language. Microsoft's cloud computing platform Azure has been existing for 5 years. In 2011 Scott Guthrie, took over the Azure team Application Platform team. The Azure user interface was then rewritten from a silver-weight application to a lightweight HTML5 web portal. During the evolution of the Microsoft Azure in 2014, it became a comprehensive, robust cloud platform for not only IaaS but also Platform-as- a-service (PaaS) cloud computing models (Cao, Wang, Li, Ren, & Lou, 2014; Madni, Latiff, Abdullahi, & Usman, 2017; Latiff, Madni, & Abdullahi, 2018; Hoang, Katz, Malozemof, 2015).

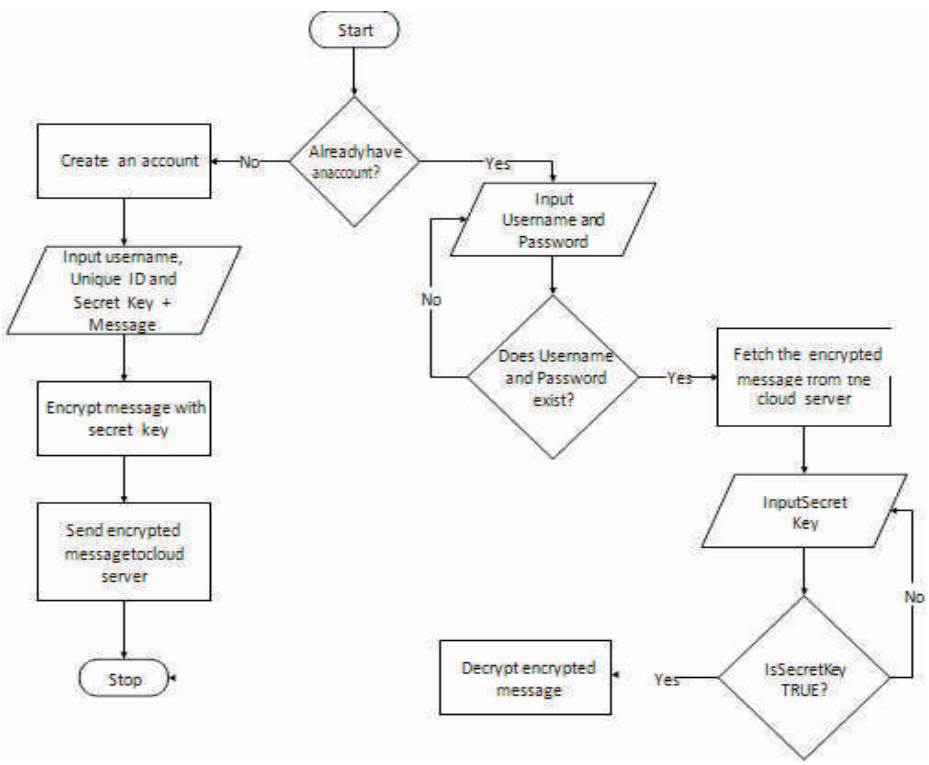


Figure 3. Flowchart of the application

5.1 Software Requirement

The software requirement used to develop this system includes C#, Microsoft Azure cloud server, Microsoft Visual Studio. The Algorithm used is Blowfish algorithm which is a symmetrickeycryptographywhichencrypt64-bitblockwith a variable length of 128-448bit

5.2 Hardware Requirement

System requirement for designing the encryption and decryption application are; 500GB hard disk, 4GB RAM, Core i3 processor.

The encryption system was implemented using Microsoft studio 2015 platform that has a Microsoft Azure sdk linked to the Azure's cloud server. The Azure cloud server allows a database to be created. The database and its tables are created on the Azure's platform with a strong internet connection. The encryption system cloud encrypt startup page has four buttons, the first requires a new user to create an account, the second allows a previous user to access a previous message, the about button gives a short description of the system is about (as shown in Figures 4 & 5).

A new cloud user is required to register with a user name and password of preference, the unique Id which serves as an extra form of authentication is generated by the system. The unique ID is required anytime the user wants to save the work in the cloud server.

Upon retrieval the message can be decrypted with the unique Id. The unique after been generated in the first step is required to be kept safe by the use because the

Figure 4. Login Page

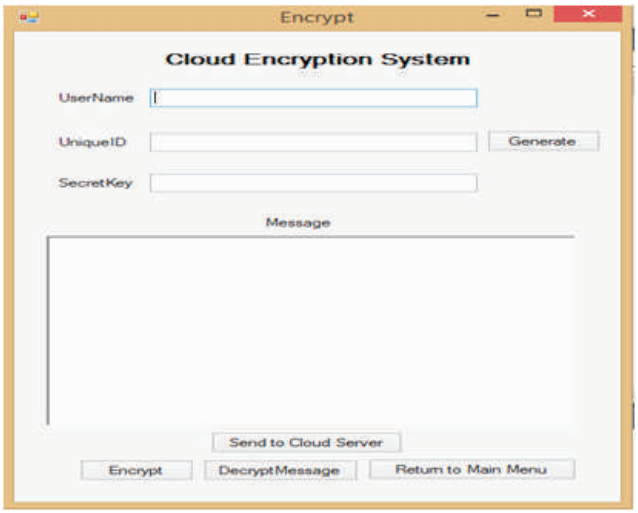


Figure 5. Encrypt Page

system cannot provide an already generated unique ID for decryption purpose. The database of the cloud encrypt system in the Microsoft Azure's platform indicates a table of IDs, username, unique Id and ciphertext. The system was first tested with a plaintext message and used to encrypt another message before it is stored in the database.

6. Performance Evaluation

6.1 Throughput

Throughput indicates the number of transactions per second or a ratio of an application handling, its amount of transactions produced over time during a test. In data transmission, network throughput is the amount of data moved successfully from one place to another in a given

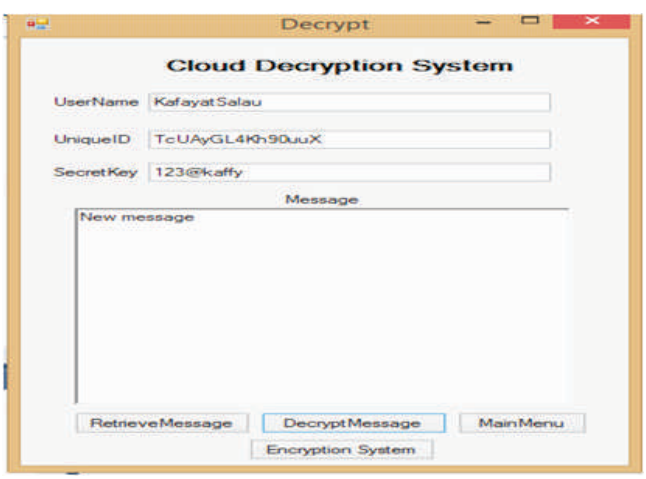


Figure 6. Decryption Page

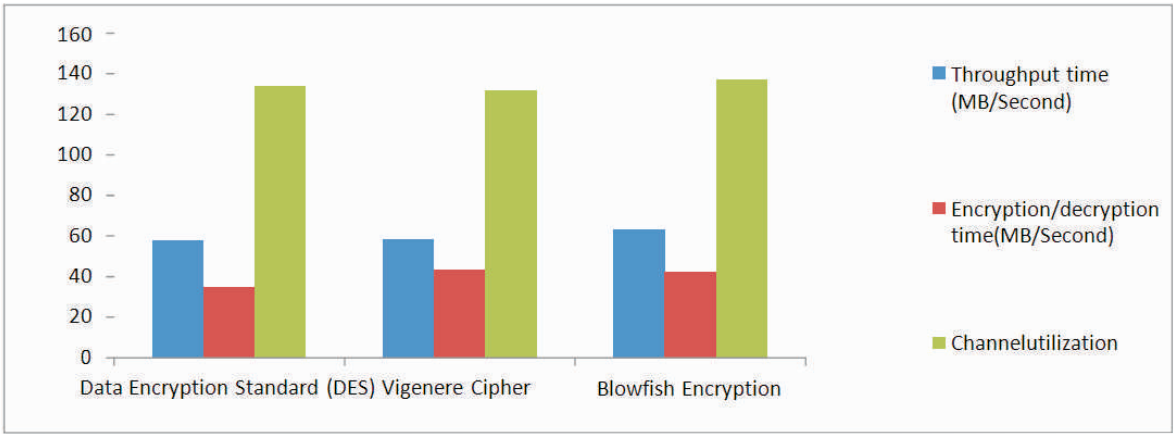


Figure 7. Evaluation Results

time period, and typically measured in bits per second (bps), as in megabits per second (Mbps) or gigabits per second (Gbps) (Madni, Latiff, & Coulibaly, 2017).

6.2 Encryption/decryption time

Encryption/decryption time defines the amount of time used to encrypt information from a sender point and the time used for decryption of same information at the receiver point (Singh, & Singh, 2013).

6.3 Channel Utilization

Channel utilization refers the channel efficiency and packet drop rate in percentage are less ambiguous terms. The channel efficiency, also known as bandwidth utilization efficiency, is the percentage of the net bit rates (in bit/s) of a digital communication channel that goes to the actually achieved throughput (Madni, Latiff, & Coulibaly, 2017).

Conclusion and Recommendations

The result of the encryption system shows data in kilobyte can be encrypted and stored in a database created in a Microsoft azure (cloud) platform. The blowfish algorithm helps the user to generate a unique Id for encrypting message (m) and same key is used to retrieve the data from the cloud. The unique Id serves as a form of authentication used for retrieval of data. The application ensures that no two party can have same unique Id and each user must keep the unique Id secret along with the chosen secret key by the user. The unique Id further helps a user in accessing stored data and decrypting it upon retrieval.

Cloud environment has provided an on-demand,pay-per- use storage services for users which enables users to access data stored in the cloud from any part globe over the internet. The cloud environment also has with it some demerit which includes loss of governance, lock-in capabilities, isolation failure, compliance, management interface failure amongst others. The developed application enables a user to incorporate an extra level of security by encrypting the data before sending it to a cloud environment. The application enhances ease of use of the encryption algorithm and guarantees efficiency of the encryption.

The developed system in its entirety is designed to encrypt message and sent to the cloud server, it also enables decryption upon retrieval. The system can be used by individual user to encrypt text message of choice before sending to the cloud environment. This paves way for easy storage data and encryption of the stored data.

References

[1]. Latiff, M. S. A., Abdul-Salaam, G., & madni, S. H. H. (2016). Secure scientific applications scheduling technique for cloud computing environment using global league championship algorithm. PloS one, 11(7), pp.158102.

[2]. Xia, Z., Wang, X., Sun,X., & Wang, Q (2016) A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data," in *IEEE Transactions on Parallel and Distributed Systems*. 27(2), pp. 340-352.doi: 10.1109/TPDS.2015.2401003

[3]. Rittinghouse, J. W., & Ransome, J. F. (2016). Cloud computing: implementation, management, and security. CRC press.

[4]. Abdullahi, M., & Ngadi, M. A. (2016). Symbiotic Organism Search optimization based task scheduling in cloud computing environment. *Future Generation Computer Systems*, 56, 640-650.

[5]. Said, A. (2005, September). Measuring the strength of partial encryption schemes. In Image Processing, 2005. ICIP 2005. *IEEE International Conference on* (Vol. 2, pp. 1126-1129). IEEE.

[6]. Kaur, M., & Singh, R. (2013). Implementing encryption algorithms to enhance data security of cloud in cloud computing. *International Journal of Computer Applications*, 70(18).

[7]. Krishnamurthy, G. N., Ramaswamy, V., Leela. G. H., & Ashalatha, M. E (2008). Blow-CAST-Fish: A New 64-bit Block Cipher. *International Journal of Computer Science and Network Security (IJCSNS)*, 8(4), pp.282.-290

[8]. Thakur, J., & Kumar, N. (2011). DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis. *International journal of emerging technology and advanced engineering*, 1(2), 6-12.

[9]. Chaplot, V (2015). Databases Management Systems (DBMS). *International Education and Research Journal (IERJ)* 1(2), pp. 24-25.

[10]. Gahi, Y., Guennoun, M.., Khatib, K. E (2000). A Secure Database System using Homomorphic Encryption Schemes Institute of Technology, 2 (1). pp.1-5.

[11]. Curino, C., Jones, E. P., Popa, R. A., Malviya, N., Wu, E., Madden, S & Zeldovich, N. (2011). Relational cloud: A database-as-a-service for the cloud.Information Applications, 1(1)pp. 0-6.

[12]. Itani, W., Kayssi, A., Chehab, A (2009) Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures IEEE International Conference on Dependable, Autonomic and Secure Computing, 3(5), (pp. 711-716) https://doi.org/10.1109/DASC.2009.139

[13]. Li, M., Yu, S., Cao, N., & Lou, W. (2011, June). Authorized private keyword search over encrypted data in cloud computing. In *Distributed Computing Systems (ICDCS), 2011 31st International Conference on* (pp. 383-392). IEEE.

[14]. Schneier, B (n.d) The Blowfish Encryption Algorithm (Blogpost) Retrieved from https://www.schneier.com/academic/blowfish/

[15]. Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Abdullah, G., Khan, S. U (2015). The rise of big data on cloud computing: Review and open research issues," *Information Systems*, 47(7) pp. 98-115. https://doi.org/10.1016/j.is.2014.07.006

[16]. Lee, C. C., Chung, P. S., & Hwang, M. S. (2013). A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments. *IJ Network Security*, 15(4), 231-240.

[17]. Cao, N., Wang, C., Li, M., Ren, K., & Lou, W. (2014). Privacy-preserving multi-keyword ranked search over encrypted cloud data. *IEEE Transactions on parallel and distributed systems*, 25(1), 222-233.

[18]. Madni, S. H. H., Latiff, M. S. A., Abdullahi, M., & Usman, M. J. (2017). Performance comparison of heuristic algorithms for task scheduling in IaaS cloud computing environment. PloS one, 12(5), pp.0176-321.

[19]. Latiff, M. S. A., Madni, S. H. H., & Abdullahi, M. (2018). Fault tolerance aware scheduling technique for cloud computing environment using dynamic clustering algorithm. *Neural Computing and Applications*, 29(1), 279-293.

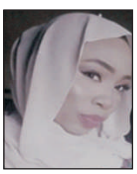
[20]. Hoang, V. T., Katz, J., Malozemof, A. J (2015). Automated Analysis and Synthesis of Authenticated Encryption Schemes," *IET Technology Security*, 3(1), pp. 1–31.

[21]. Madni, S. H. H., Latiff, M. S. A., & Coulibaly, Y. (2017). Recent advancements in resource allocation techniques for cloud computing environment: a systematic review. *Cluster Computing*, 20(3), 2489-2533.

[22]. Singh, P., & Singh, K. (2013). Image encryption and decryption using blowfish algorithm in Matlab. *International Journal of Scientific & Engineering Research*, 4(7), 150-154.

ABOUT THE AUTHORS

Shafi'i Muhammad Abdulhamid is a Senior Lecturer and Head of Department (HOD) of Cyber Security Science, Federal University of Technology Minna, Nigeria. He is also supervising both Masters and Ph.D students (in both Nigeria and Malaysia). He received his Ph.D in Computer Science from University of Technology Malaysia (UTM), M.Sc in Computer Science from Bayero University Kano (BUK), Nigeria and a Bachelor of Technology in Mathematics with Computer Science from the Federal University of Technology (FUT) Minna, Nigeria. He has been appointed as an Editorial board member for Big Data and Cloud Innovation (BDCI) and Journal of Computer Science and Information Technology (JCSIT). He has also been appointed as a Reviewer of several ISI and Scopus indexed International Journals. He has also served as Program Committee (PC) member in many National and International Conferences. He is one of the pioneer instructors at the Huawei Academy of FUT Minna and a holder of Huawei Certified Network Associate (HCNA). He is as well a member of IEEE Computer Society, International Association of Computer Science and Information Technology (IACSIT), Computer Professionals Registration Council of Nigeria (CPN), International Association of Engineers (IAENG), The Internet Society (ISOC), Cyber Security Experts Association of Nigeria (CSEAN) and Nigerian Computer Society (NCS). His current research interests are in Cyber Security, Cloud Computing, Soft Computing, Internet of Things Security, Malware Detection and Big Data. He has published many academic papers in reputable International journals, conference proceedings and book chapters.



Nafisat Abubakar Sadiq is a Graduate of Computer Science (Cyber Security Science option) from the Federal University of Technology (FUT) Minna, Nigeria. Her current research interests are in Cyber Security, Cloud Computing, Soft Computing and Big Data.

Abdullahi Mohammed is a Lecturer in Ahmadu Bello University, Zaria Nigeria. He received his B.Tech Degree in Mathematics with Computer from Federal University of Technology, Minna Nigeria. He received his M.Sc. degree in Computer Science from Ahmadu Bello University, Zaria Nigeria. He received his Ph.D in Computer Science from Universiti Teknologi Malaysia. His research interests include Algorithm Design for Distributed Systems, Big Data Analytics, Machine Learning, and Large Scale Optimization using Nature in Spired Algorithms. He is a member of IEEE and ACM..

Nadim Rana is working as a Senior Lecturer in the Department of Information Technology and Security, Jazan University, Jazan, K.S.A. He is also pursuing Ph.D. in Computer Science at Faculty of Computing, Universiti Teknologi Malaysia (UTM), JohorBahru, Malaysia. He is also a member of the Pervasive Computing Research Group (PCRG) at FC, UTM. He received his Bachelor and Master Degree in Computer Science from B.N.M. University and Hamdard University, New Delhi, India. He has published several research articles in International indexed Journals and Conferences. His research interests are in Cloud Computing, Cloud Security, Design of Scheduling Techniques using Metaheuristic Algorithms, Machine Learning and Data Mining.

Haruna Chiroma is a Senior Lecturer at the Federal College of Education (Technical), Gombe, Nigeria and also a Faculty of Computer Science and Information Technology, University of Malaya. He received his B.Tech and M.Sc Degree in Computer Science from Abubakar Tafawa Balewa University, Bauchi, Nigeria and Bayero University Kano, Nigeria, respectively. He received his Ph.D. from the Department of Artificial Intelligence. He has published over 100 articles relevant to his research interest in International referred Journals, edited Books, Conference proceedings and local Journals. He served in Technical Programme Committee of several international conferences. His main research interest includes Meta-Heuristic Algorithms, Soft Computing, Big Data, Data Mining, Machine Learning, Human Computer Interaction, Software Engineering, Information Security and Recently, Social Media In Education. He is a member of the ACM and IEEE.

Dada Emmanuel Gbenga is currently an Academic Staff of the Department of Computer Engineering, University of Maiduguri, Nigeria. He got his M.Sc (Computer Science) degree from University of Ibadan in 2009 and Ph.D degree in Computer Science in 2016 from the Department of Artificial Intelligence, University of Malaya, Malaysia. His research interests include Soft Computing Techniques and Machine Learning Algorithms with their Applications to Image Segmentation, Swarm Robotics, Information Security and Big Data.