ISSN: 2454-1907
DOI: https://doi.org/10.29121/ijetmr.v6.i12.2019.471

IJETMR
International Journal of Engineering Technologies and Management Research
A Knowledge Repository

HYBRIDIZATION OF RSA AND BLOWFISH CRYPTOGRAPHY ALGORITHMS FOR DATA SECURITY ON CLOUD STORAGE

Isiaka O.S. [1], Murtala K. [2], Ibraheem A.F. [3], Bolaji-Adetoro D.F. [4]
[1, 2, 4] Department of Computer Science, Institute of Information and Communication Technology, Kwara State Polytechnic, Ilorin-Nigeria
[3] Department of Mass Communication, Institute of Information and Communication Technology, Kwara State Polytechnic, Ilorin-Nigeria

Abstract:
Security is provided for data according to the requirements of client. Cloud computing provides different types of services. Apart from the advantages of cloud, it has many security related issues. The topmost challenge in cloud is data security. There are more possibilities that the data are accessed by the other users of cloud storage. Data security must be addressed in the cloud storage. Cryptography is the most known technique for securing the data by encryption. It is necessary to propose encryption techniques which are suitable for cloud storage. Every cloud computing provides the different level of security. The aim of this study is to improve on the security of data or file stored on cloud storage using hybrid cryptographic algorithms for encryption. The algorithms are designed in such a way that one authenticates the authorized user and the other provides confidentiality and security for data stored on cloud.

Keywords: Cryptography; Blowfish Algorithm; Cloud Storage; Data Security; Symmetric Algorithm; Asymmetric Algorithm.

Cite This Article: Isiaka O.S., Murtala K., Ibraheem A.F., and Bolaji-Adetoro D.F.. (2019). "HYBRIDIZATION OF RSA AND BLOWFISH CRYPTOGRAPHY ALGORITHMS FOR DATA SECURITY ON CLOUD STORAGE." *International Journal of Engineering Technologies and Management Research,* 6(12), 29-34. DOI: 10.29121/ijetmr.v6.i12.2019.471.

1. Introduction

Recently, cloud computing is used to generate large amount of data in daily life to store huge amount of data in different fields. Cloud computing provides different types of services to the user. The concerns of cloud computing are data security, authentication, integrity and confidentiality (Rimal et al., 2009). In order to provide the solution to these security issues on cloud storage, different algorithms and techniques have been introduced by different researchers but all with their own merits and demerits (Swathi and Bhaludra, 2017).

Cloud computing storage is used to store data and the user can access that data any time at any place. Nowadays large amount of data is stored on cloud, but majority are not secure, which gives room for unauthorized access. To provide the security to data on cloud, cryptography algorithms are most ideal (Mukhopadhyay, 2013).Cryptography is a process in which data are

ISSN: 2454-1907
DOI: 10.5281/zenodo.3595252

stored securely on cloud and transmit it in unreadable form so only authorized person can access the data (Fortine, Michael and George, 2017). Cryptography algorithm can be seen in two types. There are symmetric algorithms which uses same secret key for data encryption and decryption. Examples are: AES, DES, IDEA, TDES and Blowfish. There are also asymmetric algorithms which uses two keys: public key for data encryption and private key for data decryption. Examples are: RC6, RSA and ECC (Jasleen and Sushil, 2015).

Cloud computing offers many benefits, but is vulnerable to threats. As the use of cloud computing increases, it is likely that more criminals will find new ways to exploit system vulnerabilities. Many underlying challenges and risks in cloud computing increase the threat of data compromise (Buyya et al., 2011). Using the internet for communication and transportation of hardware, software and networking services to clients poses a serious concern about cloud computing since data management in cloud is provided by third-party. This is also because it is always a risk to handover the sensitive information to cloud service providers.

To mitigate the threat, different combination of cryptography algorithms is used in this research to provide a new type of security on cloud storage such as data security, verification and authentication. RSA algorithm gives a high level of security to data as well as provides data confidentiality (Ramalingam and Sharmila, 2015). Secure communication and user authentication is done using Blowfish algorithm. So, only an authorized person can upload/download the data on cloud. Encrypted data is stored on cloud so that an unauthorized person cannot access data from cloud (Ramalingam and Sharmila, 2015). In this proposed system, no unauthorized user can access secure data on cloud because two different cryptography algorithms are run at different places in the cloud.

2. Methodology

Cloud storage architecture with data creator and data user designed in our research is as shown in figure 1.0. If data creator wants to share the data on cloud, he/she first covert the original plain text into cipher text using a combination of RSA and Blowfish algorithms. Cipher is uploaded on cloud. So, only an authorized user can access the sensitive data. If a user wants to download data from cloud, that user has to specify authentication details. If authentication details are matched with database, then that user is authorized and will have access to original plain text.

The encryption of data uploaded is done by combining the properties of RSA and Blowfish algorithms while the decryption is done through the same properties but in reversing order in which the two algorithms are applied. Combining the two algorithms increases total time required for processing because hybridization of the two algorithms has increased run-time for both encryption and decryption. The methodology of the proposed system as in figure 2.0 examined reliability and efficiency of hybridizing RSA and Blowfish algorithms based on the performance parameters which include encryption time, decryption time, through put and delay time on different file sizes.

ISSN: 2454-1907
DOI: 10.5281/zenodo.3595252

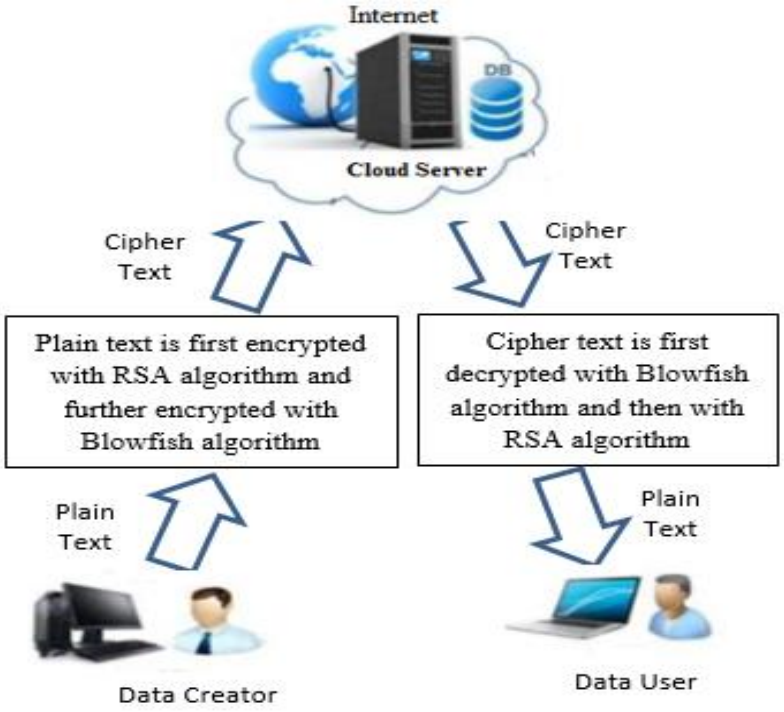

Figure 1.0: Proposed Cloud Computing Architecture

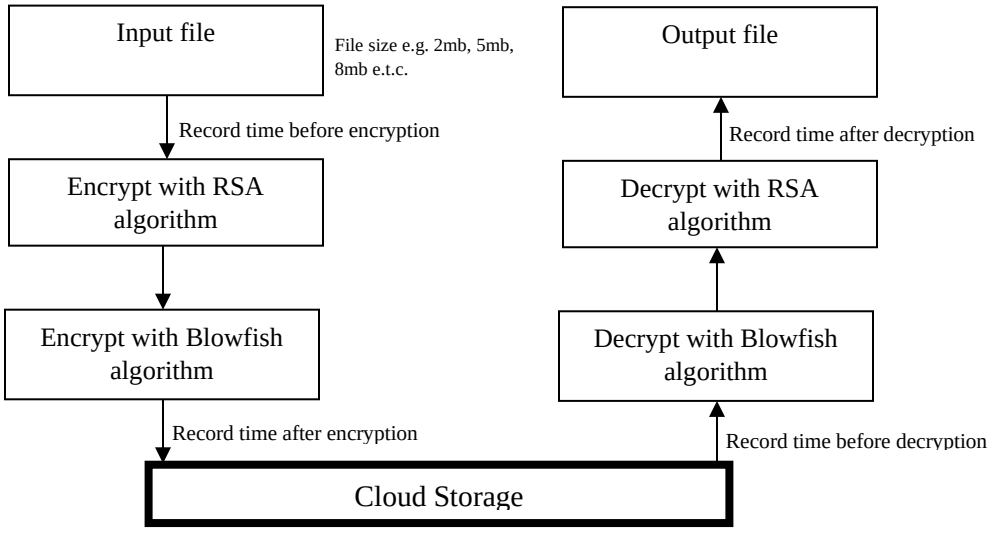

Figure 2.0: RSA and Blowfish Algorithms for data security on cloud

The parameters are evaluated as follows:

1) Encryption Time is the time taken to encrypt file by the server. Its standard measured in nanoseconds. Encryption Time = Record time after Encryption – Record time before Encryption
2) Decryption Time is the time taken to decrypt file by the server. Its standard measured in nanoseconds. Decryption Time = Record time after Decryption – Record time before Decryption

ISSN: 2454-1907
DOI: 10.5281/zenodo.3595252

3) Throughput is the rate at which data or file is transfer. It is the size of file uploaded divided time it takes to recover the file. It is measured in bytes per sec
   Throughput = size of file uploaded /delay time
4) Size of file is the size of file uploaded into server. Its standard measured in bytes.
5) Delay time is the difference between decryption time and the encryption time. It is measured in nanoseconds.
   Delay Time = Decryption Time – Encryption Time

3. Result and Discussions

The efficiency of this proposed system is determined to be efficient and reliable since the sizes of input file and output file are the same, and the throughput values of tested files with different sizes are tend towards one. The proposed system is structured to work with the standard software development procedures. It is web-based and has a relational database structure for storing the various activities involved. The Encryption system is placed in PHP codes for online access alongside with MySQL database. Figure3.0 to figure 7.0 shows the designs for encryption and decryption using the two algorithms as well as sample of encrypted files output.

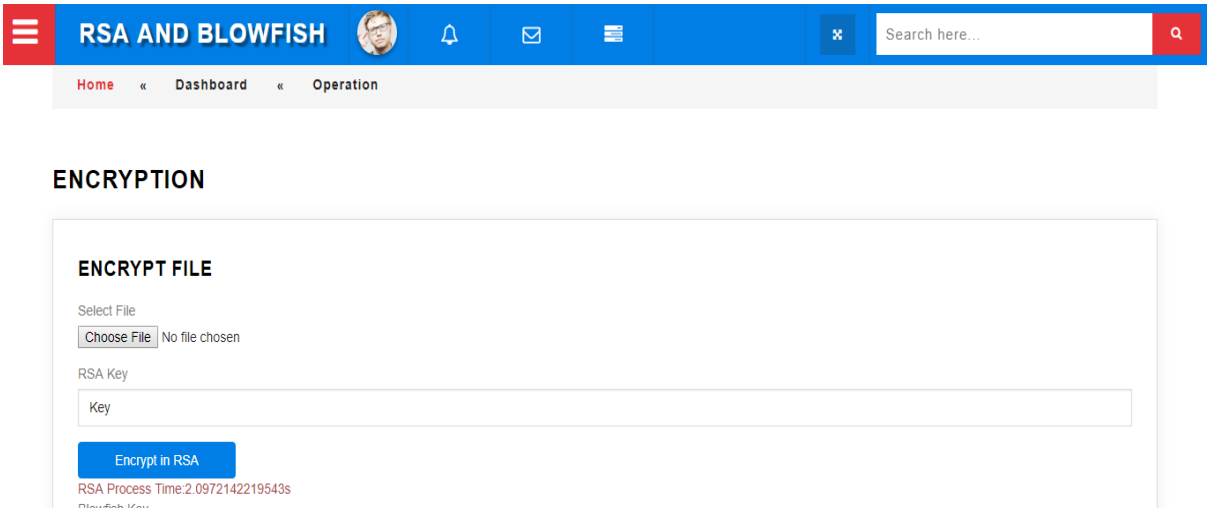

Figure 3.0: RSA Encryption Module with Process Time

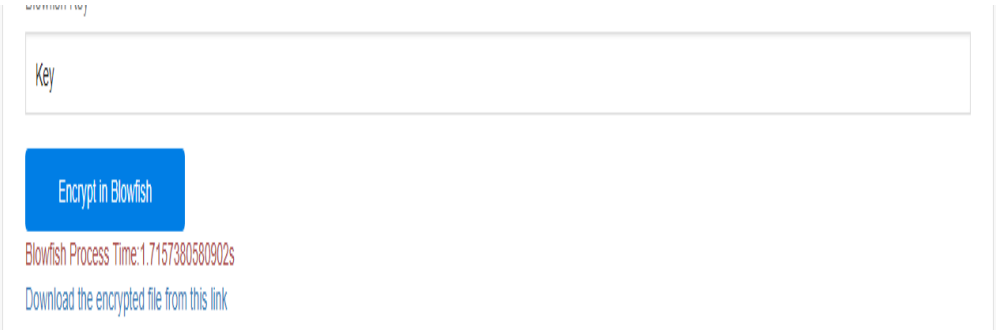

Figure 4.0: Blowfish Encryption Module with Process Time

ISSN: 2454-1907
DOI: 10.5281/zenodo.3595252

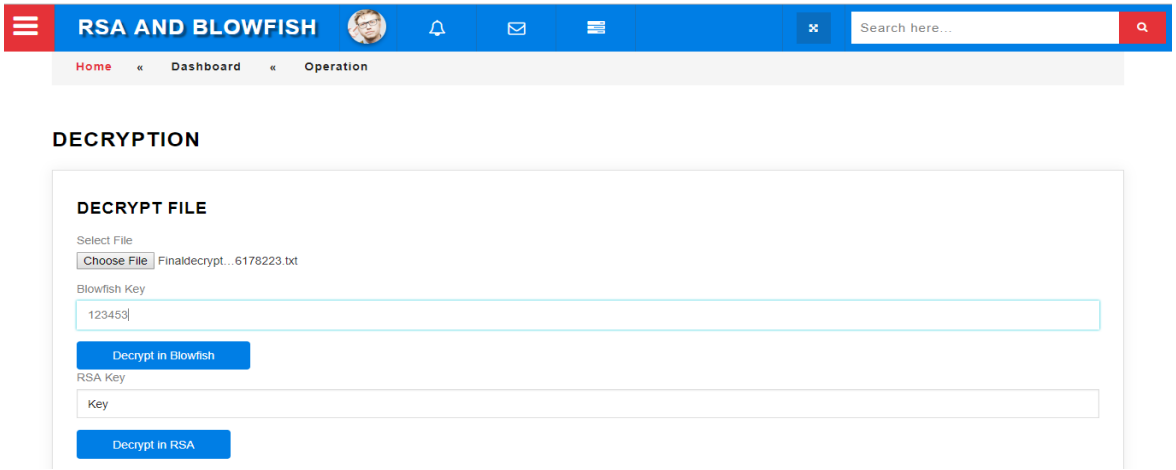

Figure 5.0: Blowfish Decryption Module with Process Time

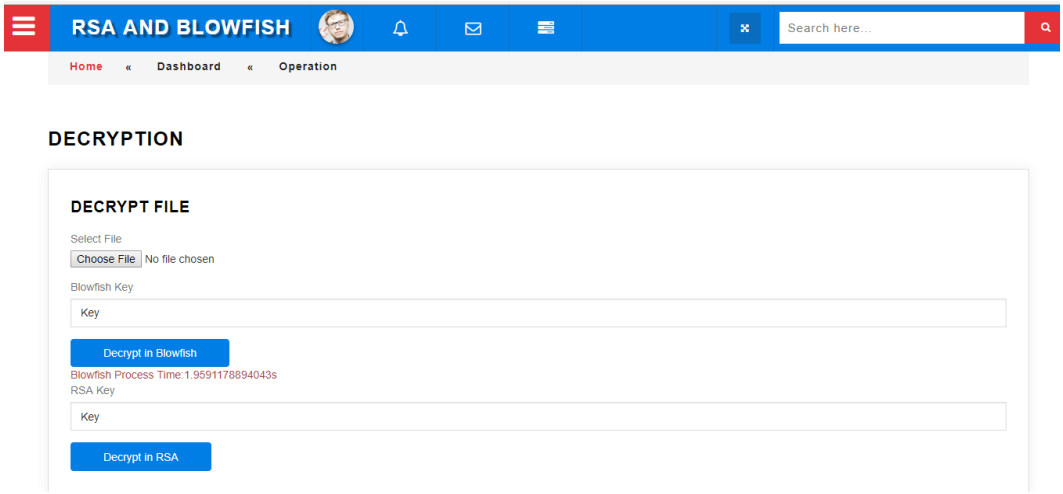

Figure 6.0: RSA Decryption Module with Process Time

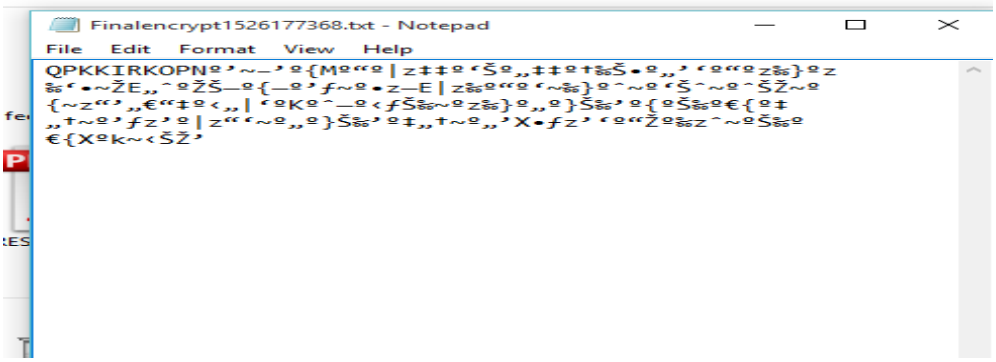

Figure 7.0: Sample of Encrypted File Output Time

ISSN: 2454-1907
DOI: 10.5281/zenodo.3595252

4. Conclusion

Cloud computing technology is widely used by different users to share data through different machines so that the data outsourced on cloud can easily be accessed. The need for all outsourced data to be on single physical machine is to transfer among users securely. To preserve privacy in cloud is an important aspect cloud computing in order to safe guide the identity of users. So far that anyone can share data on cloud, the most important aspect of cloud computing is to keep the data safely and securely. Though the major challenge faced in Cloud storage while saving data is security. In view of this, the proposed system assists in providing security for data stored in the Cloud with the combinations of RSA and Blowfish algorithms. Cryptography helps the user to share data in safer manner. RSA algorithm deals with authenticity and validity of data while Blowfish algorithm deals with security (Manikandan et al., 2011). From the result, it shows that the hybrid of RSA and Blowfish algorithms provide much stronger properties derived from properties of both algorithmsso as to guide against threats and prevent unauthorized users from accessing our data.

References

[1] Aayushi P., Rana Y.K. and Patel B.P. (2015). "Design and Implementation of an Algorithm to Enhance Cloud Security". International Journal of Computer Applications (0975 – 8887) volume 113 – No. 12.

[2] Buyya R. et al. (2011). "Introduction to Cloud Computing". Cloud Computing Principles and Paradigms. John Wiley & Sons.

[3] Fortine M., Michael K. and George O. (2017). "Enhanced Secure Data Storage in Cloud Computing Using Hybrid Cryptographic Techniques (AES and Blowfish)". International Journal of Science and Research (IJSR), Volume 6 Issue 3. Available on www.ijsr.net, accessed on 23/10/2019.

[4] Jasleen K. and Sushil G. (2015). "Security in Cloud Computing using Hybrid of Algorithms". International Journal of Engineering Research and General Science Volume 3, Issue 5. Avaialable online at www.ijergs.org, accessed on 2/11/2019.

[5] Manikandan G. et al (2011). "A Hybrid Approach for Security Enhancement by Modified Crypto-Stegno Scheme". European Journal of Scientific Research, vol. 2, pp 206 – 212.

[6] Mukhopadhyay D. (2013). "Enhanced Security for Cloud Storage using File Encryption". Proc. International Conference on Distributed Computing and Internet Technologies.

[7] Ramalingam S. and Sharmila B.S. (2015). "Symmetric Encryption Algorithm to Secure Outsourced Data in Public Cloud Storage". Indian Journal of Science and Technology, Vol 8 (23), D OI: 10.17485/ ijst/ 2015/ v8i23/ 79210. Available online on www.indjst.org, accessed on 25/10/2019.

[8] Rimal B. et al. (2009). "A Taxonomy and Survey of Cloud Computing Systems". Proc. Fifth International Joint Conference on INC, IMS and IDS, pp: 44 – 51, held at Korea.

[9] Swathi B. andBhaludra R.S. (2017). "Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm". International Journal of Advance Research in Science and Engineering, volume No. 06, Issue No. 11 pp 70 – 77. Available online at www.ijarse.com, accessed on 2/11/2019.

*Corresponding author.
E-mail address: isiakaosalman2@ gmail.com/ kabeermurtala@ gmail.com/ alabi043@ yahoo.com, bolajiadetorofunsho@ gmail.com