International Journal of Science and Advanced Innovative Research
ISSN: 2536-7315 (Print) 2536-7323 (Online)
Volume 7, Number 3, September 2022
http://www.casirmediapublishing.com

Secure File Storage on Cloud Computing Using Hybrid Cryptography

Mohammed Ali Bizi[1*] & David T. Oladipo[2]
[1]Department of Computer Science, Federal Polytechnic Damaturu, Yobe, Nigeria
[2]Department of Computer Science, Federal Polytechnic Damaturu, Yobe, Nigeria
Email: *bizi002@yahoo.co.uk

ABSTRACT
Customers can now access resources and services globally using cloud computing from any location at any time. The majority of network traffic consists of data, both multimedia and non-multimedia, which has high computing and memory requirements as well as security restrictions. Technology-based devices like computers and smartphones have constrained resources as well as unreliable data integrity and confidentiality. As a result, the requirement for safe storage in a cloud-computing environment becomes apparent. This research work presented secure file storage in a cloud-computing environment using a hybrid cryptography technique. The system has been designed based on combined AES, RSA, and TWOFISH approach. The new proposed system was evaluated. The experimental results show the hybrid algorithms have much better performance in terms of file security and time management for both encryption and decryption.
Keyword: Cloud Computing, Hybrid Cryptography, AES, RSA, TWOFISH, Algorithm File Storage

INTRODUCTION
Presently, security is a global phenomenon which draws the attention of governments, stakeholders, corporate society as well as individuals to make available, a bearable protection mechanism for good, though security as it sounds may perhaps not be a singleton, it requires several layers of protection to ensure effectiveness. Therefore, the need for securing file storage on the cloud is very essential. Literature review uncovered relative existing systems such as Secure file Storage on Cloud using Cryptography (Selvanayagam, *et al,2018,* Poduval, *et al, 2019* & Kumar, *et al, 2020*), Design of Secure Storage for Health-care Cloud using Hybrid Cryptography(Chinnasamy, *et al,2018*), Hybrid Cryptography based E2EE for Integrity & Confidentiality in Multimedia Cloud Computing(Harnal, *et al, 2019*) among others which worth basing on upside purposes. Cryptography is a field for such a scenario, that transform an actual data into Cipher text such that one and only one user has the right to access the data using the appropriate

key from the cloud storage server. Cryptography is aimed at providing a protection mechanism for file storage against unauthorized users. Symmetric key based (private-key) and asymmetric key-based (public-key) are the two categories of algorithms used in cryptography. In the former, the same key is applicable for encipher and decipher, and this technique is been used by AES, DES, 3DES, RC2, TWOFISH, and BLOWFISH algorithms. While the later employ different keys for encipher and decipher as adopted by ELGAMMAL and RSA algorithms.

Cloud computing as mentioned by the National Institute of Standard and Technology (NIST) is an approach that allows the convenient and demand network base access to configurable and valuable computing resources (e.g storage, server , network, software and services) (Peter et al, 2011; Harnal et al, 2016). Cloud computing is one of the internet-based architecture, where several computing and storage services are provided through the Service Level Agreement (SLA). As such, many organizations find it easy to utilize those services at cheaper rate from the cloud service provider (e.g Google Apps, Salesforce, Amazon's and windows Azure) at anytime and anywhere base on pay per usage as against the offline services. The utilization of those cloud service required high level protection for data confidentiality, integrity and availability (Harnal et al , 2019).

Today, data stores with cloud service providers are liable to the following challenges:

- Lack of data availability, which occurs as a result of server failure or crash from the cloud service provider, makes it difficult for a user to access.
- Lack of data integrity occurs because of failure to protect the data in the cloud against accident and deliberate alteration without authorization.
- High risk of data leakage, including the malicious hack of cloud providers or compromises of cloud user accounts.

Given these mentioned challenges, our work intends to provide a secure mechanism for file storage on the cloud using a hybrid cryptography approach.

Related work

Bansal et al (2015), proposed an approach for securing data using a hybrid encryption algorithm (i.e RSA and Blowfish). Field Programmable Gate Array (FPGA) was employed to ensure data integrity and confidentiality. The approach of Akomolate et al (2017), employed the use of a hybrid cryptography algorithm (i.e AES, Blake2b and Schnorr signature) for data security on cloud storage. Navdeep Singh et al (2015), employed the use of data encryption and decryption through AES and RSA algorithms. In this approach, data is encrypted on the client side before delivery on the cloud. The authors (Chinnasamy et al, 2018), proposed an approach using a hybrid cryptography algorithm (i.e Blowfish and Enhance RSA) for securing storage on the cloud. Their approach provides fast encryption, large prime numbers for key generation and efficient key management. The approach of the authors (Poduval et *al, 2019*), employed a hybrid cryptography algorithm (i.e AES, 3DES, and RC6) for securing storage on the cloud. In their framework, LSB techniques were used to provide a secure key for storage on the cloud. Selvanayagam et al (2018), proposed an approach for securing file storage on the cloud using cryptography algorithm (i. e AES, DES and RC2). Elliptic Curve Cryptography (ECC) was employed to ensure data integrity and confidentiality.

However, the use of a single key for encryption and decryption is a major drawback. Swathi et al (2017), proposed a model for securing file storage in cloud computing using a hybrid cryptography algorithm (i.e. Blowfish and SRNN). In this model, half breed encryption is employed such that records are scrambled by blowfish combined with document part and SRNN maintain for the secured correspondence between clients and servers. The approach of Hernal et al (2019), proposed a hybrid cryptography algorithm based End-To-End (E2EE) approach for maintaining integrity and confidentiality of multimedia in a cloud computing environment. This work has provided a secure storage and transmission of multimedia files across the internet with high level of integrity and confidentiality. Rawal et al (2017), proposed a framework that provide secure storage on the cloud through separated servers based on user input, storage and output request. In this approach, three separate servers are used to prevent data failure and improved security. Kanatt et al (2020), proposed an approach for securing file storage in the cloud using hybrid cryptography algorithm (AES, RSA and Blowfish). In their approach, comparison was made between AES and RSA, AES and blowfish for encryption and decryption to determine the best approach. From their finding, AES and blowfish prove to be more secure compared to AES and RSA. In this work, a hybrid cryptography algorithm will be used similar to the approach of Kanatt *et al (2020)*. However, our proposed approach is distinct by using AES, RSA and TWOFISH for securing storage in the cloud computing environment so as to have better improvement.

System Design

The design of the system is based on multi-media and non-multi-media files taken from students' data using a hybrid cryptography algorithm for ensuring file security. The proposed work was carried out in three sequential steps as user account creation, file upload and download. In the first step a user signs up for account creation using his valid details, file is chosen by the user for upload and a combined encryption algorithm (AES, TWOFISH and RSA) was used to secured the selected file. Finally, the user decrypted the file using the key to obtained the original message through download as shown in figure 1,

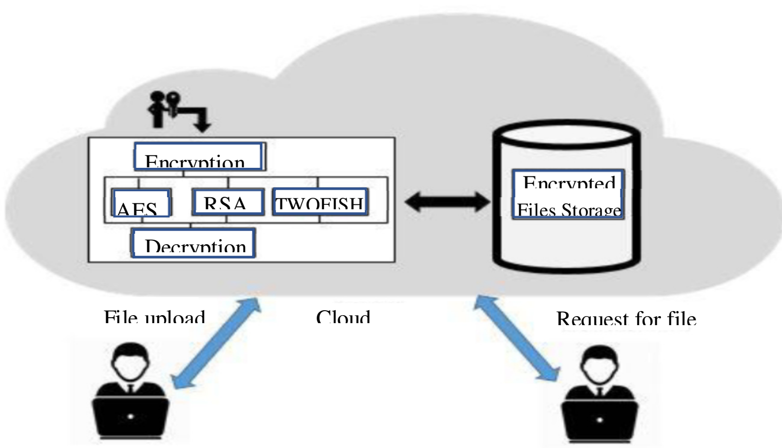


Figure 1: Model description of the overall system

A. AES Algorithm

The Advance Encryption Standard (AES) is a symmetric-key cipher algorithm founded by Vincent Rijmen and Joan Daeman. AES consist of

International Journal of Science and Advanced Innovative Research
ISSN: 2536-7315 (Print) 2536-7323 (Online)
Volume 7, Number 3, September 2022
http://www.casirmediapublishing.com

key length of 128-bit block cipher with 128,192 and 256 bits' key sizes. The AES design is based on a Substitution Permutation Network (SPN) and does not use the Data Encryption Standard (DES) feistel network, thus making it stronger and faster than Triple-DES(Kanatt *et al 2020*).The AES algorithm is currently the best, because in addition it is also safe for the encryption and decryption process is very fast. Santoso(2019) mention the following as AES encryption and decryption procedures shown in figure 2 :

1) Key identification
2) Give the first logical value of turns and sum the key of the first rotation.

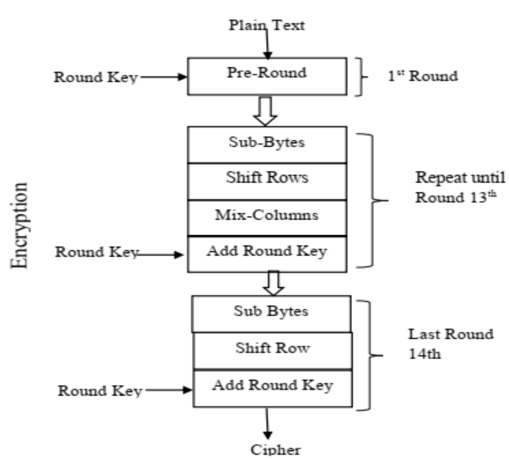
3) Rounds = 1 to 13: with Sub Bytes, Shift Rows, Mix Columns, Add Round

4) KeyFor the last round without Mix Coloums.

5) The encryption output depend on the round 14.

Four basic steps constitute every round:

1) Sub Bytes
2) Shift Rows
3) Mix Columns
4) Add Round Key



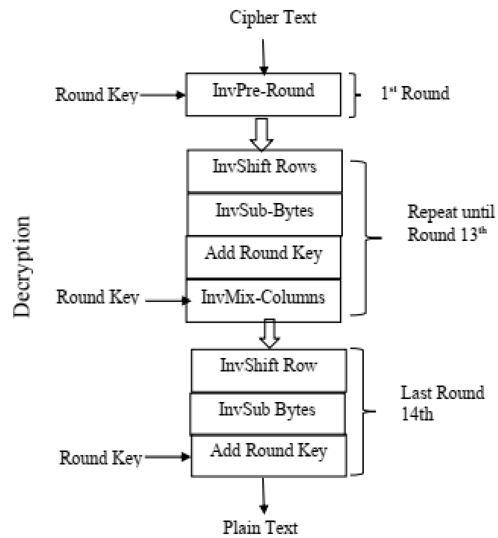


Figure 2: AES procedure

B. TWOFISH Algorithm

Twofish was developed by Bruce Schneier in 1998 and is 128-bit symmetric block cipher algorithm that allow a variable-length key. The cipher is a 16-round network with a bijective F function made up of four key-dependent 8-by-8-bits S-boxes, a fixed 4-by-4 maximum distance separate matrix. In the twofish algorithm, the input and output data are XOR-ed with eight sub-keys ko……k7. Santoso(2019) mention the following as Twofish procedures shown in figure 3 :

1) P Plaintext is split into four segments of 32 bits each.
2) Four keywords are XORed with this in the whitening input stage.
3) A sixteen-round procedure is used. The function g receives the two words on the left in each round as input.
4) The linear mixing step based on the MDS matrix is followed by S-boxes that depend on the provided key bytes in the g function.
5) Every S-box generates an 8-bit output and requires an 8-bit input.
6) A 4X4 MDS matrix is multiplied by the four results, which are sent as vectors of length 4.
7) Two keywords are added when the Pseudo-Hadamard Transform (IPM) is used to merge the output of the two functions g.
8) The letters "XOR" are then exchanged between these two results (one of which is opened by the first 1 bit, which is played after that).

9) After that, the left and right are switched for the following round.
10) Following the completion of all rounds, the last round switch is reversed, and empathy is XORed with four additional keywords to produce cypher text.

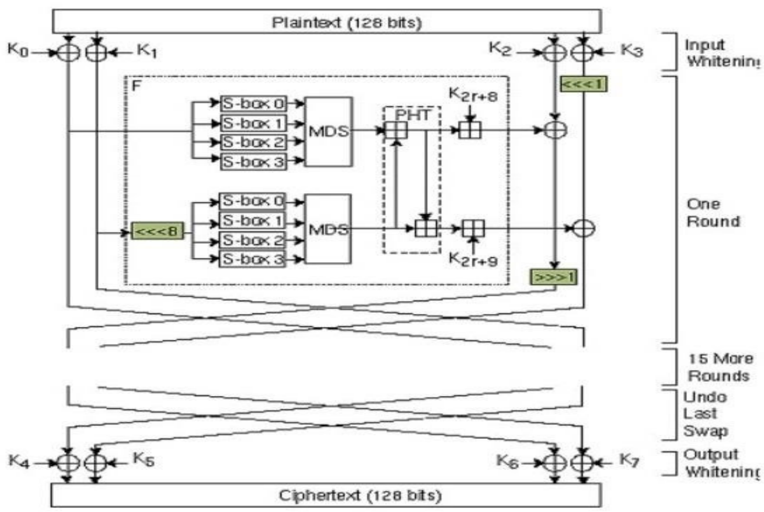


Figure 3: Twofish procedure

C. RSA Algorithm

In the RSA (Rivest-Shamir-Adleman) algorithm, the modular operation is the fundamental operation. Asymmetric public-key encryption techniques like RSA are among the most widely used and safe. The algorithm takes advantage of the fact that very big (100–200 digit) values cannot be factored effectively. The difficulty of modulus operation depends on number of division operations involved which can be reduced by using Montgomery modular multiplication algorithm, one of the fastest algorithms to find the modular multiplication for large numbers. The complexity of a modulus operation is determined by the number of division operations required, which can be decreased by utilizing the Montgomery modular multiplication algorithm, one of the quickest methods for determining the modular multiplication of big integers. Kanatt *et al (2020)* mention the following as RSA procedures shown in figure 4

RSA procedure with encryption key as (e,n):

Set message to be whole number from 0 to (n1). Broke- down larger messages to generate number of blocks in the same level of integer.

1. Encrypt message with the eth power modulo n
2. Decrypt message with the power d modulo n.

The (e,n) is assign to public and the (d,n) is assign to private key

The e,d and n are obtain as:

1. Select two larger (100+-digit) prime numbers as p and q.
2. Let n = p * q.
3. Select integer d, where GCD(d, ((p-1) * (q1))) = 1
4. Calculate e as e * d = 1 (mod ((p-1) * (q-1)))

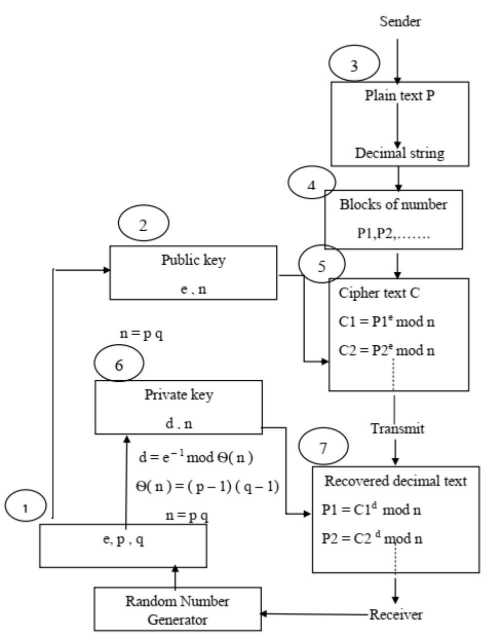


Figure 4: RSA procedure

D. HYBRID APPROACH

In this approach, the combined cryptography algorithm (AES, Twofish and RSA) was used to secured file storage in the cloud. Step1, the user initiated the original message and encrypted with AES follow by Twofish using same key size of 128 because of the symmetric nature of algorithm;

International Journal of Science and Advanced Innovative Research
ISSN: 2536-7315 (Print) 2536-7323 (Online)
Volume 7, Number 3, September 2022
http://www.casirmediapublishing.com

then later encrypted with RSA using key size of 1024 exchange because of the asymmetric nature to generate complex message. This process is called top-down encryption process. Step2, name as bottom-up decryption process, the complex message decrypted with asymmetric algorithm(RSA) using key and further decrypted with symmetric algorithm (AES and Twofish) to produced back the original message. The overall process is shown in figure 5.

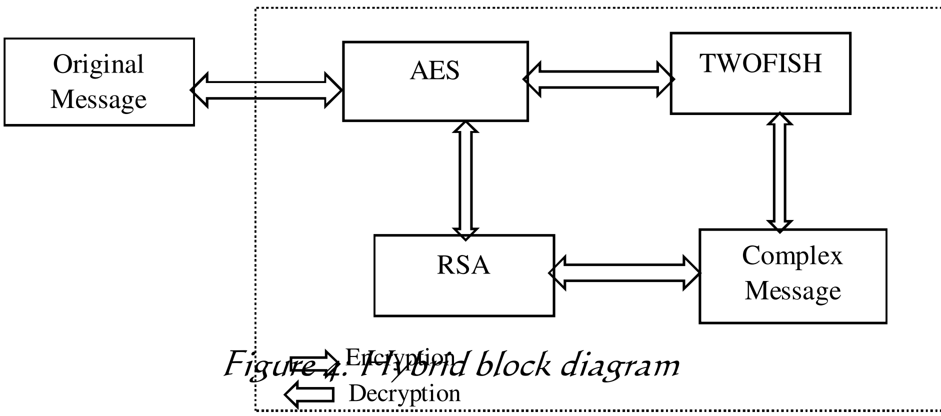


Figure 4: Hybrid block diagram

IMPLEMENTATION

The research work was implemented with PHP version 7.2.1, mysql 5.0.12, Apache 2.4.29 for AES, RSA, TWOFISH and the Hybrid algorithm. The experiments are carryout in Int^{R} Core ^{TM} i5 CPU @ 2.30GHz processor, 8GB RAM, Window 10, 64bit operating system. Default setting of PHP are used for the experimental environment.

RESULT

Result analysis can be described as an essential stage that needs the understanding of all the activities under investigation (Valerie, 1996). The objective of the experiment is to investigate the performance of Hybrid cryptography (AES, RSA. TWOFISH) algorithm to secured file storage in the cloud. In this experiment, user initiated an original file(imagefile1(2).png) and the uploaded file is encrypted using the hybrid cryptography algorithm, which result to complex message as shown in figure 5. In addition, the file was decrypted by user using the key to obtained back the original message through download as shown in figure 6. The encryption and decryption time comparison for various input size file are provided in Table (I - II), and figure (7 - 8).

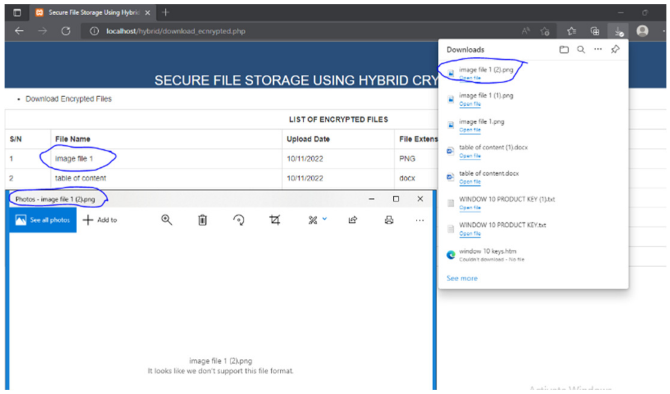


Figure 5: Experiment for File Encryption

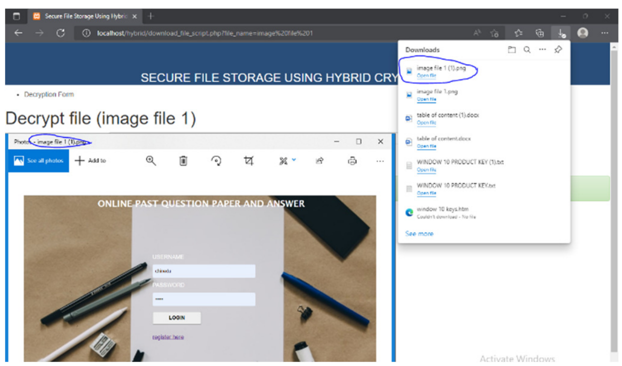


Figure 6: Experiment for File Decryption

Table I: Encryption Time Comparison

Encryption Table						
Filename	Date	Size	AES Encipher Time (Milliseconds)	RSA Encipher Time (Milliseconds)	Twofish Encipher Time (Milliseconds)	Hybrid Encipher Time (Milliseconds)
asp_done.docx	2022/11/24 11:32 PM	771.14 KB	2.98	3.07	3.65	1.67
Batch_File_to_Reset_Windows_Update.zip	2022/11/24 11:32 PM	3.17 KB	2.24	2.27	2.30	2.21
CamScanner 11-15-2022 10.38	2022/11/24 11:33 PM	15.39 KB	3.05	3.68	3.77	1.75
VID-20221119-WA0026_551b.mp4	2022/11/24 11:33 PM	573.00 KB	2.28	3.20	3.68	1.40
View Chart						

International Journal of Science and Advanced Innovative Research
ISSN: 2536-7315 (Print) 2536-7323 (Online)
Volume 7, Number 3, September 2022
http://www.casirmediapublishing.com

Table II: Decryption Time Comparison

Decryption Table

Filename	Date	Size	AES Decipher Time (Milliseconds)	RSA Decipher Time (Milliseconds)	Twofish Decipher Time (Milliseconds)	Hybrid Decipher Time (Milliseconds)
asp_done.docx	2022/11/24 11:32 PM	771.14 KB	2.48	2.49	2.49	0.64
Batch_File_to_Reset_Windows_Update.zip	2022/11/24 11:32 PM	3.17 KB	0.77	0.78	0.78	0.02
CamScanner 11-15-2022 10.38	2022/11/24 11:33 PM	15.39 KB	1.67	2.10	2.10	0.55
VID-20221119-WA0026_551b.mp4	2022/11/24 11:33 PM	573.00 KB	2.08	2.22	2.23	0.64

View Chart

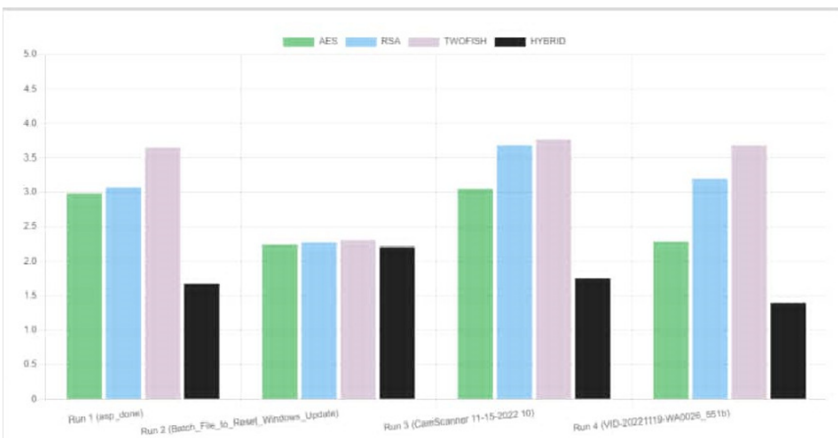


Figure 7: Multiple Bar Chart for Encryption Comparison

As shown in Figure 7 (Multiple Bar Chart), at run1, the hybrid algorithms encrypt file(asp_done.docx) with size of 771.14kb at the time 1.07 ms, compare with AES at time 2.98 ms, RSA at time 3.07 ms and Twofish at time 3.07ms. Also at run 2, the encryption time for the hybrid algorithm is 2.21 ms for the file (Batch_file_to_Reset_windows_update.zip) with size 3.17kb, compare with AES at 2.24ms, RSA at 2.77ms and Twofish at 2.30ms. The hybrid algorithm encryption time for the file (Camscanner11-15-2022-10.38) is 1.75ms with 15.39kb at run 3. Also at run 4, the hybrid algorithm encrypt file (VID_20221119-WA0026_551b.mp4) with 573.00kb at 1.40ms, compare to AES at 2.29secs, RSA at 3.20ms and Twofish 3.68ms.

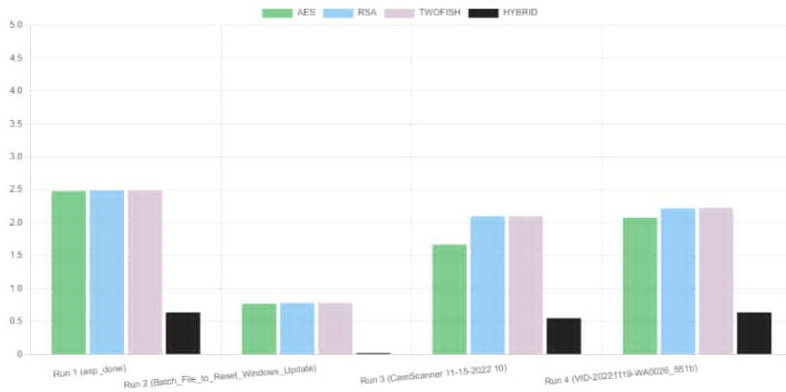


Figure 8: Multiple Bar Chart for Decryption Comparison

As shown in Figure 7 (Multiple Bar Chart), at run1, the hybrid algorithms decrypt file(asp_done.docx) with size of 771.14kb at the time 0.64 ms, compare with AES at time 2.48 ms, RSA at time 2.49ms and Twofish at time 2.49m s. Also at run 2, the encryption time for the hybrid algorithm is 0.02 ms for the file (Batch_file_to_Reset_windows_update.zip) with size 3.17kb, compare with AES at 0.77ms, RSA at 0.78secs and Twofish at 0.78ms. The hybrid algorithm encryption time for the file (Camscanner11-15-2022-10.38) is 0.55 ms with 15.39kb at run 3. Also at run 4, the hybrid algorithm encrypt file (VID_20221119-WA0026_551b.mp4) with 573.00kb at 0.64ms, compare to AES at 2.08ms, RSA at 2.22ms and Twofish 2.23ms. Based on the graphical analysis of figure (7 – 8), it is clearly observed that the hybrid algorithms have much better performance in terms of file security and time management for both encryption and decryption.

CONCLUTION

This research work has presented a secure file storage on cloud computing using hybrid cryptography algorithms. The system has been implemented using an algorithm based on AES, RSA and TWOFISH. The experimentation on the hybrid algorithm resulted in better performance in terms encryption and decryption time. The work also provides an accurate and effective means of securing file on the cloud. Such an automated system can be used in application where file security is a major challenge.

REFERENCES

Harnal, S., & Chauhan, R.K (2019). Hybrid Cryptography base E2EE for Integrity & Confidentiality in Multimedia Cloud Computing. International Journal of Innovative Technology and Exploring Engineering (IJITEE). Vol. 8, No. 10. ISSN: 2278-3075. PP. 918-924. DOI:10.35940/ijitee.J9001.0881019. www.ijitee.org

Kanatt, S., Jadhav, A. & Talwar, P. (2020). Review of Secure File Storage on Cloud using Hybrid Cryptography. International Journal of Engineering Research & Technology (IJERT). Vol. 9, No. 02. ISSN: 2278-0181, PP. 16 -20. http://www.ijert.org

K.I Santoso, M. A Muin & M. A Muhmudi. (2019). Implementation of AES Cryptography and Twofish Hybrid Algorithm for Cloud. Journal of Physics: Conferences Series 1517(2020)012099 DIO:10.1088/1742-6596/1517/012099. IOP Publishing

Kumar, U., & Prakash, J. (2020).Secure File Storage on Cloud using Hybrid Cryptography Algorithm. International Journal of Creative Research Thoughts(IJCRT). Vol. 8, No.7. ISSN: 2320-2882. PP. 334 – 340. www.ijcrt.org

Navdeep S.& Pankaj D. K. (2015). A Hybrid Approach for Encrypting Data on Cloud to prevent DoS Attacks, International Journal of Database Theory and Application Vol. 8, No. 3, PP. 145-154, http://dx.doi.org/10.14257/ijdta.2015.8,3,12

Oladeji, P. A., & Matthew, O. A. (2017). A Hybrid Cryptographic Model for Data Storage in Mobile Cloud Computing, International Journal of Computer Network and Information Security, Vol.6, PP. 53-60.

Chinnasamy, P., & P., Deepalakshmi(2018). Design of Secure Storage for Health-care Cloud Using Hybrid Cryptography. Proceeding of the 2nd International Conference on Inventive Communication and Computaional Technology (ICICCT). ISBN: 978-1-5386-1974-2 PP. 1708-1711. Doi:10.1109/ICICCT2018.8473107

Peter Mell, Timothy Grance. (2011). "The NIST Definition of Cloud Computing", NIST Special Publication.

Poduval, A., Doke A., Nemade, H. & Nikam, R. (2019). Secure File Storage on Cloud Using Hybrid Cryptography. International Journal of Computer Science and Engineering Open Access. Vol. 7(1), EISSN: 2347-2693. PP. 587-591

Rawal, B.S., & Vivek, S.S. (2017). Secure Cloud Storage & File Sharing. IEEE International Conference on Smart Cloud (Smart Cloud).

Selvanayagam, P., Singh, A., Michael J. & Jeswani J. (2018). Secure File Storage on Cloud using Cryptography. International Research Journal of Engineering and Technology (IRJET) Vol. 05, No. 03. EISSN: 2395-0056. PP. 2044-2047. www.irjet.net

Shilp Harnal, R.K. Chauham. (2016). "Multimedia Support from Cloud Computing: A Review". International Conference on Microcom -2016, IEEE,NIT Durgapor

Swathi, B. & Singh, R. B. (2017). Secure File Storage in Cloud Computing using Hybrid Cryptography Algorithm. International Journal of Advance Research in Science and Engineering (IJARSE).Vol. 06, No. 11. ISSN: 2319-8354. PP.70-77. www.ijarse.com

Bansal, V.P., & S.Singh (2015). A hybrid data encryption technique using RSA and Blowfish for cloud computing on FPGAs. 2nd International Conference on Recent Advances in Engineering Computational Sciences(RAECS), Chadigarh , pp. 1-5. Doi: 10.1109/RAECS.2015.7453367.