Hybridized Cryptographic Method for Cloud Data Storage

Simeon A. Ojo, N.D. Nwiabu, E.O Bennett
Department of Computer Science, Rivers State University, Port Harcourt, Nigeria

Abstract— This work introduces cloud computing, exploring the characteristics, service models and inherent security challenges in cloud data storage. To guard against data insecurity, a hybrid cryptographic technique called ADK (Hybrid) was proposed. A combination of Advanced Encryption Standard (AES), Blake 2b hash function and Time Based One Time Authentication Password (TOTP) authentication mechanism which is more preferred for efficient cloud data storage security and integrity. The AES algorithm uses 256bits key for providing enhanced security which is obtained through an optimized key generation module. Generating Secrete key, user file is hashed with Blake 2b to produce data hash. User login unique credentials (e-Mail address and phone number) is XORRED to give a first layer key. The data hash is XORRED with generated first layer key to generate a secrete key for the AES. The secrete key is not stored, it is generated at the point use via one-time password to authenticate against an intruder. The development stage was done using .Net Framework, C# and Microsoft SQL Database and was hosted on Cloud server. The experimental result shows that the use of a time-based one-time password, email address, mobile phone number alongside and password as the security parameters to check against an intruder was able to optimize security. The proposed system is more efficient for large data storage and retrieval from the cloud server.

Index Terms— Cloud Data Storage, Cloud Computing, Advanced Encryption Standard (AES), Blake2b, Time Based One Time Password (TOTP), Cryptography.

1 Introduction

Cloud computing is seen as the delivery of computing facilities comprising server, software, networking, storage, databases, analytics, and intelligence over the Internet for faster innovation, flexible resources, and markets of scale. The advent of cloud computing technique brought about massive and multipurpose collections of facilities which is accessible in nature based on the necessities of corporate in tallying to providing comforts for productive and instant results. It also provides the capacity to access corporate documents and shared infrastructure, proposing services on demand in a networked environment to perform processes that meet growing business needs [4].

Reference [2] in his own word define cloud computing as the collection of application software and services that can be applied via the internet rather than residing on a local personal computer or local servers. In like manner, [6] stated that Cloud computing is "a type of computing in which immensely scalable and flexible IT-enabled competencies are delivered as a service to remote customers using internet technologies". This is evident as it offers user(s) with abilities to store, process and retrieve their data from a subscribed data centres in a variety of service models such as Software as service (SaaS), Platform as a service (Paas), and Infrastructure as a service (IaaS) and in varieties of released models such as hybrid, private, community, and public.

The Security challenges attributed to cloud computing is huge. Consequently, the supplier must ensure that the facility provided is secured. Cybersecurity is seen as one of the major threats to the world today which has raised many concerns to individuals and co-operates bodies in cloud computing environments. Data theft has continued to grow and rise to an extent where organizations find new ways of data security to enable safe data transfer among others for information security [3].

In recent years, different applications based on cloud computing technologies have emerged such as remote storage, stock trading, and electricity bill payment. Such dealings, over wired or wireless public networks, required an end-to-end secured connection and information sharing which need to be confidential. In other to guarantee data is well secured, various companies have come to the comprehension that, to have a successful edge in a competitive market, significant business processes need to be integrated into the Internet.

A recent study in the field of e-business is pointing toward building a secure and efficient business procedure that integrates with diverse levels of security with reference to a level of information sensitivity [13]. The idea of Cryptography has helped to upturn the security of encrypted file which is uploaded to the cloud storage. The essence is to ensure that file encryption and decryption is done in a secure way within a very short time and maximum cost-effectiveness. Going through the process, major attacks targeted on sensitive file is being prevented [7].

This paper presents Hybrid technique named “ADK Hybrid” which is a combination of Advanced Encryption Standard (AES), Blake2b hash function and Time-Based One Time Password (TOTP) Authentication mechanism which is more preferred for efficient cloud data storage security and integrity.

1.1 Cloud Computing Model

The hereafter of computing is in the cloud. Cloud models showcase in three types: SaaS (Software as a Service), IaaS (Infrastructure as a Service) and PaaS (Platform as a Service). Each of them has it unique packages that could serve the needs of various organisation. This research explores SaaS with the below inherent benefits:

1. **Inexpensive** – SaaS is cheap as it eradicates the costs embedded with the securing, installing, maintening and upgrading of computing facility.
2. **Easy Accessibility** – SaaS provides ease of access to the services using any device and anywhere.
3. **Ease of Usage –** setting up SaaS services is very easy, just click of buttons you have your service running.

1.2 SAAS SECURITY ISSUES

In a customary on-premise application deployment model, the attributed data of each user continues to reside within the user's boundary and is subject to its physical, logical and personnel security and access control policies [24]. However, in the SaaS model, the user data is stored outside the party boundary subjecting them to the mercy of the provider for security measures.

No doubt, cloud storage user will like to have cloud storage to securely save all their valuable data meanwhile a disgruntled personnel may act as cloud administrator and access the data and destroy it or send it acros to user rivals [25]. As a result, cloud data storage security becomes at heart real issue. To this end, the user data needs to be safeguarded from the external foes and also present it unreadable to cloud administrators.

1.3 CRYPTOGRAPHY

Cryptography is required to guarantee the confidentiality and authentication of the data when attempting to migrate sensitive data to cloud data storage. [19] defined "Cryptography as the science of using mathematics for making plain text information (P) into an unreadable ciphertext (C) format called encryption and reconverting that ciphertext back to a plain text called as decryption with the set of Cryptographic Algorithms (E) using encryption keys (k1 and k2) and the decryption algorithm (D) that reverses and produces the original plain text back from the cypher text. This can be interpreted as Ciphertext C = E {P, Key} and Plain text C = D {C, Key}."

Consequently, user data and secrete key undergo a series of encoding using desired algorithms to produce the ciphertext through the process called data encryption. Similarly, the ciphertext and the secrete key are applied to produce the original data through data encryption process.

1.4 CRYPTOGRAPHIC STRUCTURES

There are some basic fields in cryptography that made the objectives of Cryptography a reality. From the lists are:

1. Encryption and Decryption: Basically, the transformation of data to ciphertext and ciphertext back to the original data. Considering encryption and decryption, the cypher starts with AddRoundKey stage which in turn followed by certain number of rounds depending on the key size and each includes all four stages, followed by the last round. The example includes AES, 3DES, Blowfish, Serpent and Arcfour [10].
2. Hashing Algorithm: This is basically the conversions which results in an n-bit product from an input of random length. They are mostly employed for proving the integrity of communicated data and a check for a sustainable goal of data integrity [10]. The example includes Blake 2b, MD4, MD5 and SHA.
3. Message Authentication Codes (MAC): According to [10], "one of the most fascinating and complex areas of cryptography is that of message authentication and the related area of digital signatures. It would be impossible, in anything less than book-length, to exhaust all the cryptographic functions and protocols that have been proposed or implemented for message authentication and digital signatures".

1.5 HYBRIDIZED CRYPTOGRAPHY

Below are the algorithms that sum up the proposed hybridized method:

1. AES: Reference [10] stated that "AES uses arithmetic in the finite field GF(28) with the irreducible polynomial m(x) = x8 + x4 + x3 + x + 1. Consider two elements A = (a7a6 c a1a0) and B = (b7b6 c b1b0). The sum A + B = (c7c6 c c1c0), where ci = ai ⊕ bi . The multiplication {02} # A equals (a6 c a1a00) if a7 = 0 and equals (a6 c a1a00) ⊕ (00011011) if a7 = 1.2 and summarily AES operates on 8-bit bytes" The encryption part has the following steps [25]:
   a) Bytes Substitution: This is the application of S-box to execute a sequential byte substitution to guard against attacks.
   b) Rows Shifting: This the is the permutation and cyclical one byte row
   c) Columns Mixing: The column are treated just like four-term polynomial which are basics in the field.
   d) Addition of Round Key: Respective byte is joined with a byte of the round key by Xorring.

   The decryption unit is simply a reverse function of the respective transformation in a reverse order with the expanded key. This then ascertain confidentiality [10].
2. Time-Based One Time Password Authentication (TOTP): This is based on HMAC based One Time Password Algorithm (HOTP) however the moving factor is time instead of the conventional counter. TOTP uses time in increments, which is about 30 or 60 seconds based on the environment of use. This implies that each of the one-time passwords is valid within the duration of the time span.
3. Blake2b: This is an improved version of SHA-3 that is rooted in the family of Blake2 algorithm. It is enhanced for 64-bit boards including NEON-enabled ARMs and generates digests of different sizes ranges between 1 and 64 bytes [26]. It is used for generating hash value in order to check for any modification in the original data.

2 RELATED WORKS

Reference [5] works on the "Architecture for Data Security in Multi-cloud Using AES-256 Encryption Algorithm" and described new architecture for the safekeeping of data stored in several cloud environment. The file is encrypted by AES and the encrypted file is split into equal parts based on the number of available cloud storage and stored accordingly. Their projected system improves data security in a multi-cloud environment. However, their approach is susceptible to the middle layer man attack at the transport layer. Also, the approach stands costly due to additional cost incurred with multi-cloud storage, no authentication and this place the approach in an unbalanced mode.

Reference [8] stated that file transfer over a network is exposed to security challenges like the hijacking of data by illicit parties. To enhance the worth of data security, the author proposes the combination of AES 256 bit algorithm and MD 5 hashing. But today, MD5 could not be seen as responsible choices for a secure hash function.

A new hybrid cryptography technique was developed by [11]. Their proposed system is tested with plain text. This is divided into two segments, each segment is encrypted using a different encryption algorithm and this is being executed simultaneously. The associated cost would be significantly high as the asymmetric cryptographic technique is involved.

Another mechanism that ensures that the file passes the test of confidentiality, integrity, and authentication by hybridizing asymmetric (RSA), symmetric (AES) algorithms and SHA256 hash functions was built by [26]. However, the execution time is significantly high for RSA, likewise, the reliability of files with SHA256 is questioned when deprived of an additional security layer.

Reference [16] uses the Advanced Encryption Standard (AES) system that encodes the image block size of 128 bits by employing three different secrete key sizes 128, 192 and 256 bits. The projected architecture uses a block size of 128 bits with 256 key sizes. The author focuses on the secret key, the yardstick that upturns the security and also the complexity of the algorithms. However, the approach lacks authentication.

3 METHODOLOGY

The methodology adopted for this study is Action Research, the team style is called a collaborative inquiry. Fundamentally, this is an on-premise operation, principally aimed to handle definite problem set up in a particular circumstance [12]. Reference [9] stated that action research encompasses minor scale interventions in the running of the real world and a close investigation of the effects of such a mediation.

The hybridized cryptographic method (ADK Hybrid) includes 256 bits key AES, Blake 2b hash function and Time-Based One Time Password (TOTP) authentication. Figure 1 shows the pictorial layout of the proposed cloud system where users from their computer device can run the ADK application and connect to the cloud storage.

To achieve a high-security standard, the user must advocate personal security that is hidden from the cloud data storage provider. This is achieved by encrypting user data locally prior upload to the cloud data storage. The method is embedded with basically two design modules as shown in Figure 2: Encryption, and Decryption. Each of the modules is integrated with the implementation of Blake2b Algorithm and Time Based One Time Password (TOTP) mechanism for authentication

3.1 Encryption Module

The Hybridized AES algorithm (ADK) uses 256bits key for providing enhanced security which is obtained through an optimized padding scheme and key generation module. This involves:

1. User Authentication: User security parameters Unique e-mail Address and Phone Number is authenticated via TOTP and Saved if a new user.
2. Terminates if authentication failed else continue.
3. Generation of private key: This is achieved in two-step:
    a) Perform XORRING on user credentials (Email Address and Password)
    b) Perform a Hash function with Blake2b on user data.
4. Perform XORRING on the result from step (3a) and 3(b). This is the Secret Key for Encryption
5. Generate Round Key from the Expansion of the Secrete Key
6. Add Round Key with the user Data
7. Perform the below AES Round 1 operation
    a) Bytes Substitution
    b) Rows Shifting
    c) Column Mixing
    d) Addition of Round Key
8. Repeat Step 7 twelve (12) more times
9. Perform the AES for the last Round Excluding Mix Column only. The ciphertext is now generated
10. Upload the Cipher Text and Hash Data

3.3 Decryption module

This design ensures that data on transit is fully encrypted. The encrypted data is retrieved from the cloud server on successful authentication of the user while it dismisses if the authentication failed. On successful retrieval, the data is decrypted locally from the user desk. The steps include:

1. User Authentication: User security parameters Unique e-mail Address and Phone Number is authenticated via TOTP and Saved if a new user.
2. Terminates if authentication failed or else go to the next step
3. Download User Hash Data and the Cipher Data.
4. Secret Key Generation: This is achieved in two-step:
   a) Perform XORRING on user credentials (Email Address and Password)
   b) Perform XORRING on Hash Data and the Result from 4(a)
5. Generated Round Key by the expansion of the secrete Key
6. Include the Round Key and the Cipher Text
7. Execute the paramount AES reverse actions:
   c) Inverse Bytes Substitution
   d) Inverse Rows Shifting
   e) Inverse Columns Mixing
   f) Addition of Random Key
8. Replicate Step 6 above twelve (12) times
9. Perform AES Inverse actions without Inverse columns mixing
10. You now have your original data.

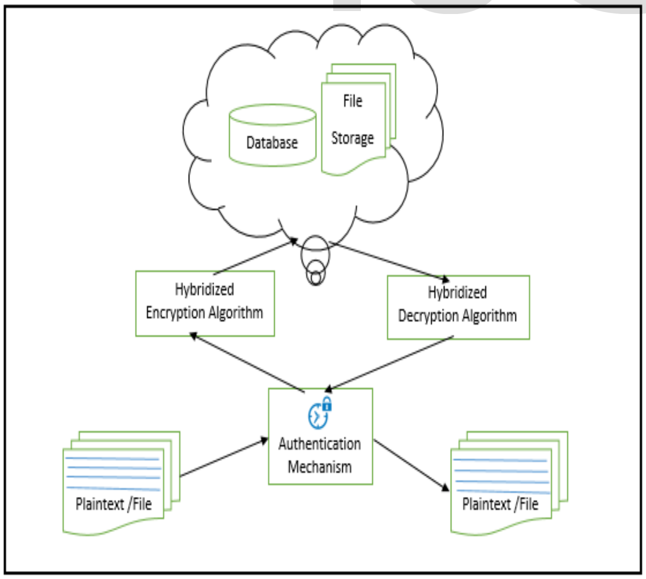

Figure 1: Pictorial layout of the proposed system

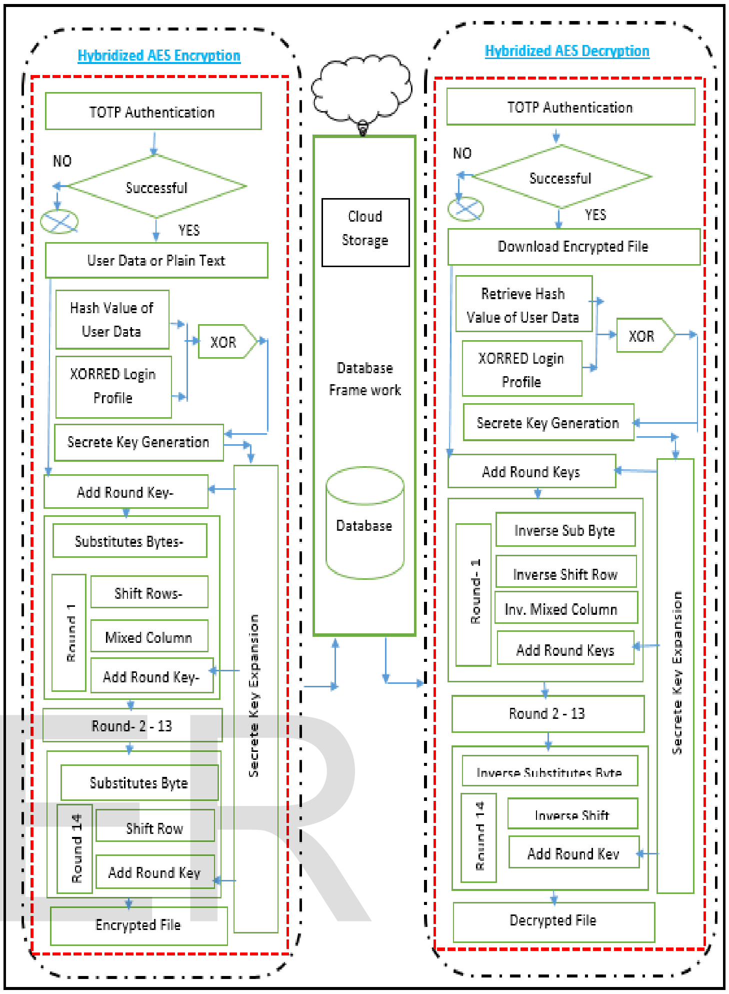

Figure 2: Hybridized ADK Architecture

4 Results and Discussion

The following algorithms – ADK (Hybrid), AES, and DES were implemented on .Net platform using Microsoft visual studio 2017 integrated development environment and tested with different sizes of the file starting from 1MB to 245MB.

The outcomes of ADK (Hybrid) were compared with the chosen algorithms (main AES and DES). The yardstick applied for the assessment is the file size before and after encryption process, the execution time for both encryption and decryption, and the throughput as shown in tables 1 to 3 and illustrated in Figure 3 to Figure 7.

The comparison of the file sizes before and after encryption of test data was evaluated as seen in table 1.

TABLE1

EVALUATION OF ORIGINAL AND DECRYPTED FILE SIZE

AES		DES		ADK Hybrid	
Default File Size (mb)	Encrypted File Size(mb)	Default File Size (mb)	Encrypted File Size (mb)	Default File Size (mb)	Encrypted File Size (mb)
1.00	1.84	1.00	2.00	1.00	1.00
10.00	19.59	10.00	20.00	10.00	10.00
20.00	39.54	20.00	40.00	20.00	20.00
40.00	79.69	40.00	80.00	40.00	40.00
55.00	109.80	55.00	110.00	55.00	55.00
75.00	149.49	75.00	150.00	75.00	75.00
110.00	219.99	110.00	220.00	110.00	110.00
120.00	239.70	120.00	240.00	120.00	120.00
160.00	319.90	160.00	320.00	160.00	160.00
170.00	339.30	170.00	340.00	170.00	170.00
200.00	398.81	200.00	400.00	200.00	200.00
245.00	489.76	245.00	490.00	245.00	245.00

Table 1 shows the results generated from the proposed hybrid system. This table captures the file size before encryption, file size after encryption for AES, DES and ADK (Hybrid) system. Both AES and DES approximately have the encrypted file doubled the original file while the hybridized ADK algorithm optimizes the size of the file by retaining the original size. This is considerably good, no extra cost is attached while uploading to the cloud server storage compared to when the encrypted file size is increased.

The associated time comparison for the proposed system with test data of different sizes is evaluated in table 2 below.

TABLE 2

SELECTED ALGORITHM EXECUTION TIME EVALUATION

File Size (MB)	AES (seconds)		DES (seconds)		ADK (seconds)	
	Encryption	Decryption	Encryption	Decryption	Encryption	Decryption
1	1.564	1.429	3.085	2.010	3.049	1.575
10	5.702	4.061	7.305	4.993	4.795	1.890
20	10.222	5.863	11.583	8.028	6.636	2.296
40	20.269	10.024	22.750	13.603	9.278	2.976
55	27.706	15.799	30.833	19.559	10.844	3.759
75	39.788	21.260	38.913	25.010	15.220	4.815
110	58.334	30.544	46.092	38.401	30.578	6.727
120	63.76	34.151	62.735	45.830	21.097	7.019
160	83.626	42.460	110.528	45.446	27.413	9.482
170	75.648	49.081	118.172	46.722	28.996	9.306
200	99.070	51.063	126.592	55.971	33.156	10.684
245	107.572	65.896	147.278	90.619	40.109	12.979

Proposed ADK Hybrid was optimized to handle large file size for efficient upload to cloud data storage.

For file size less than 10MB, ADK did significantly close to AES but better than DES considering the execution time.This is clearly pictured in Figure 3 and Figure 4 respectively. On the good side for the ADK Hybrid, there is a significantly high performance from file Size 10MB upward. Remarkably, ADK performs much faster than both AES and DES and the results show the greater the file size, the higher the time of execution for both AES and DES.

The execution times for Hybridized ADK encryption and Decryption is represented as shown in Figure 3. The results show that the execution time for both encryption and decryption increases as the file size increases. Approximately, the encryption to decryption ratio ranges from 3.21 to 1.02

Figure 4 compared the time elapsed for the encryption using AES, DES and ADK algorithm. ADK did noticeably high for file size ranges from 10MB upward.

.

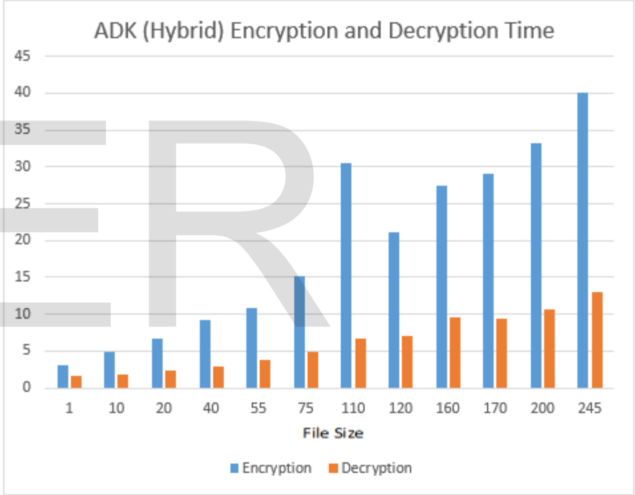

Figure 3. ADK (Hybrid) Time of Execution Time

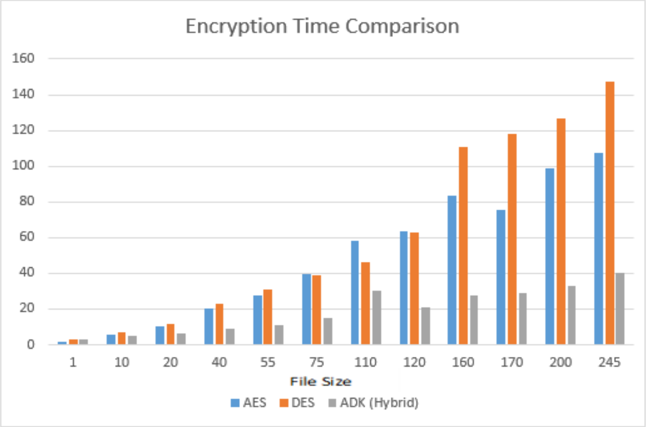

Figure 4. Encryption Time Comparison

The execution time for decryption is compared and is represented in Figure 5 below

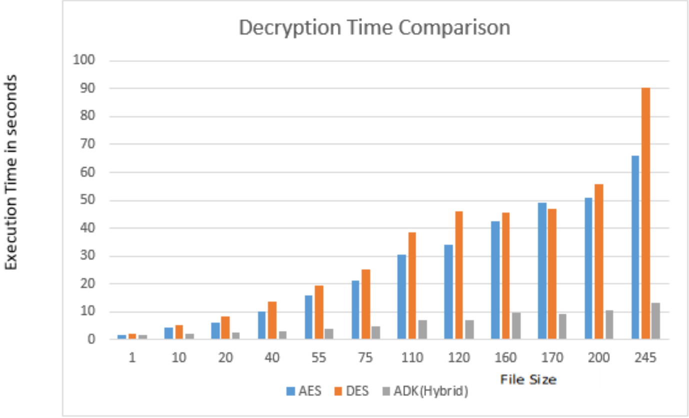

Figure 5. Decryption Time Comparison

Table 3 shows the outturn (Mb/Secs) execution with AES, DES and ADK (Hybrid) considering both encryption and decryption. This is also known as throughput.

TABLE 3
OUTTURN/THROUGHPUT ANALYSIS FOR AES, DES AND ADK (HYBRID)

	File size per unit time of execution (MB/S)					
File Size (MB)	AES		DES		ADK (Hybrid)	
	Encryption	Decryption	Encryption	Decryption	Encryption	Decryption
1	0.639	0.7000	0.324	0.498	0.328	0.635
10	1.754	2.4623	1.369	2.003	2.086	5.291
20	1.957	3.411	1.727	2.491	3.014	8.711
40	1.973	3.990	1.758	2.941	4.311	13.441
55	1.985	3.481	1.784	2.812	5.072	14.632
75	1.885	3.528	1.927	2.999	4.928	15.576
110	1.886	3.601	2.387	2.865	3.597	16.352
120	1.882	3.514	1.913	2.618	5.688	17.096
160	1.913	3.768	1.448	3.520	5.837	16.874
170	2.247	3.463	1.439	3.639	5.863	18.268
200	2.018	3.917	1.580	3.573	6.032	18.720
245	2.278	3.718	1.664	2.704	6.108	18.877

The File size per unit time of execution of the algorithms is calculated using [18]:
Throughput = T_P / E_T
Where T_P is the size of the file in megabytes (MB) and E_T is the time of execution.

Figure 6 and Figure 7 shows the encryption throughput and decryption throughput respectively for AES, DES and ADK. Results show that ADK has better throughput than both AES and DES. Likewise, AES delivered a good outturn than DES during encryption except for a noticeable drop on a file size 110MB which is applicable to ADK as well. For decryption throughput, AES and DES have a relatively close performance.

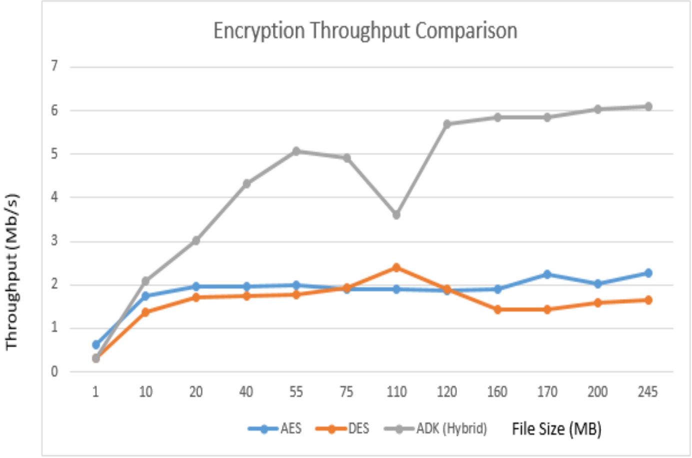

Figure 6. AES, DES and ADE Throughput Relationship - ENCRYPTION

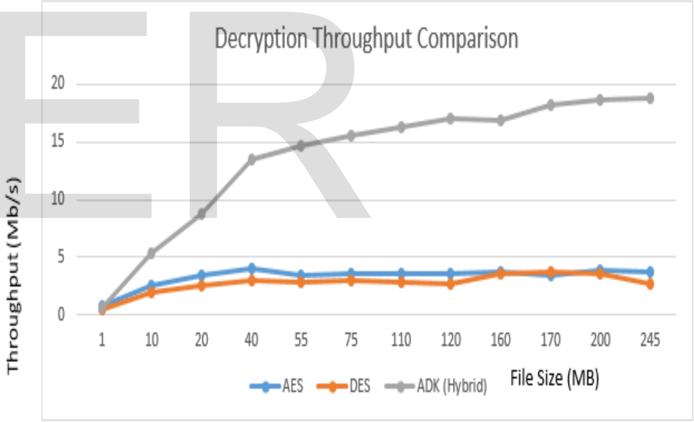

Figure 7. AES, DES and ADE Throughput Relationship - DECRYPTION

5 CONCLUSION

Having seen the need to protect data in the cloud with any choice cryptographic algorithm, the cost implication of the chosen algorithm cannot be relegated. The only way to cost maximization is to maximize the execution time and also ensure the file size after encryption is relatively the same if not smaller the original file size for efficient fast upload and management of the subscribed cloud data storage. In this paper, a strong and cost-efficient authentication based hybridized algorithm was proposed to ensure that the user need not worry about associated cost due to increased file size as seen with other algorithms, encryption and decryption key, a secrete key is securely generated uniquely for each file so as to mitigate against inherent security challenges that may accompany format-preserving encryption (FPE) standard.

With this approach, confidentiality, Integrity, and authentication is guaranteed on cloud data storage.

REFERENCES

[1] V.Masthanamma,G.Lakshmi Preya "An Efficient Data Security in Cloud Computing Using the RSA Encryption Process Algorithm" 2015

[2] Stroh, & Kumar;(2009) The Cloud is Ready for you,Are you ready for Cloud?Retrieved

[3] Laney, D. (2001) 3D Data Management Controlling Data Volume, Velocity and Variety, Information Systems International Journal of Advanced Research in Computer and Communication Engineering 47 116-124.

[4] Agrawal, D., Das, S., & El Abbadi, A. (2011). Big data and cloud computing. In Proceedings of the 14th International Conference on Extending Database Technology - EDBT/ICDT '11 (p. 530). New York, New York, USA:ACM Press. doi: 10.1145/1951365.1951432

[5] Rashmi S. Ghavghave, Deepali M. Khatwar "Architecture for Data Security In Multicloud Using AES256 Encryption Algorithm" International Journal Recent and Innovation Trends in Computing and Communication Volume: 3 Issue: 5 ISSN: 2321-8169

[6] Gartner, T (2012). Contributing factors of cloud computing adoption a Technology organization environment framework approach. International Journal of Information Systems and Engineering 1(1), pp.38–49.

[7] Anjanachaudhary, ravinder Thakur, manishmann", A review: data security approach in cloud computing by using RSA algorithm", International Journal of Advance Research in Computer Science and Management Studies, volume 1,Issue 7, December 2013

[8] Hendra Pasaribu, Delima Sitanggang, Rudolfo Rizki Damanik, Alex Chandra Rudianto Sitompul, "Combination of advanced encryption standard 256 bits with md5 to secure documents on android smartphone" 2018

[9] Walliman, N. (2001) A Step by Step Guide for the First Time Researcher. Sage, Thousand Oaks.

[10] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, ISBN 978-0-13-444428-4, Pearson Education, 2017.

[11] Ali Abdulridha Taha1, Diaa Salama Abd Elminaam1 and Khalid M. Hosny (2018) "An Improved Security Schema for Mobile Cloud Computing Using Hybrid Cryptoraphic Algorithms"

[12] Clarke, R. J. (2005) Research Methodologies, Agenda Definition

[13] Chi Sung-Do, Park Jong, Jung Ki-Chan and Lee, Jang-Se (2001) Network Security Modeling and Cyber Attack Simulation Methodology

[14] S. Subashini, and V. Kavitha. (2010) "A survey on security issues in service delivery models of cloud computing." J Network ComputAppldoi:10.1016/j.jnca.2010.07.006. July, 2010.

[15] Padmapriya, Dr.A, Subhasri, P. (2013) "Cloud Computing: Security Challenges & Encryption Practices". International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 3, pp. 257.

[16] Sneha Ghoradkar,Sneha Ghoradkar, "Review on Image Encryption and Decryption using AES Algorithm", 2015

[17] Peltier and Thomas, (1993) Designing information security policies that get results. Info security news 4(2), 30-31.

[18] N. Nagar and U. Suman, ―A secure mobile cloud storage environment using encryption algorithm‖, International Journal of Computer Applications, vol. 140, no. 8, pp. 0975 – 8887, April 2016.

[19] Akashdeep Bhardwaja, GVB Subrahmanyam , Vinay Avasthi , Hanumat Sastry ―Security algorithms for cloud computing‖, Procedia Computer Science, vol. 85, pp. 535-542, 2016.

[20] Sreekanth, G. Shakeeba S. Khan, R. and Tuteja R. (2015): Security in Cloud Computing using Cryptographic Algorithms, International Journal of Innovative Research in Computer and Communication Engineering 3(1), 66-78.

[21] Ku Sankalpa N. Moharir, "A Review in Advanced Encryption Standard (AES) Algorithm on FPGA", 2015

[22] KINCHELOE, J. L. Teacher formation as a political commitment: mapping the postmodern. Porto Alegre Medical Arts, 1997

[23] Seyed Hossein Kamali and Reza Shakerian, "A Modified Advanced Encryption Standard Algorithm for Image Encryption

[24] C. Lakshmi Devi, D. Kanyakumari, Dr K. Venkataramana Security issues in SaaS of cloud computing

[25] A. Sachdev and M. Bhansali, ―Enhancing cloud computing security using AES algorithm‖, International Journal of Computer Applications, vol. 67, no. 9, 2013.

[26] Jean-Philippe Aumasson, Samuel Neves, Zooko Wilcox-O'Hearn, and Christian Winnerlein4 BLAKE2: simpler, smaller, fast as MD5

[27] N. M. AbdElnapi, F. A .Omara, and N. F. Omran, ―A hybrid hashing security algorithm for data storage on cloud Computing‖, International Journal of Computer Science and Information Security, vol. 14, no. 4, pp. 175, 2016.

AUTHORS' PROFILES

Simeon A. Ojo obtained B.Tech in Computer Science from Ladoke Akintola University of Technology, Ogbomoso, Nigeria in 2012 and currently pursuing MSc. in Computer Science from Rivers State University, Port Harcourt, Nigeria. His research interests include Cloud Computing, Big Data Analytics, Data Mining, IoT, Software Engineering. He has been managing both on-premise and cloud data for both public and private sectors across Nigeria especially in the hospitality industry and can be reached at simeonabiodunojo@yahoo.com.

Dr N. D.Nwiabu pursued Bachelor of Science from Kwame Nkrumah University of Science & Technology, Kumasi, Ghana in 2002, and Master of Science from University of Port Harcourt, Nigeria in 2006. He also obtained PgCert in Research Methods and PhD from Robert Gordon University, Aberdeen, UK in 2009. He is currently working as a lecturer in Department of Computer Science, Rivers State University, Nigeria since 2012. He is a member of IEEE computer society since 2011, a member of NCS since 2005 and CPN since 2005. He has numerous publications and conference papers in reputed international journals including IEEE. His main research work focuses on Situation-aware system, Pipeline monitoring, Decision support system, prediction system, etc. His work won awards in the North Sea, IEEE, MIT, and EIM. His work has also got an application area *in sociology to monitor crime. He has 16 years of teaching experience and over 10 years of Research Experience.*

Dr. E.O Bennett pursue Bachelor of Science from Rivers State University, Nigeria. He also obtain PgCert and PhD from the University of Port Harcourt, Nigeria. He is currently working as a lecturer in the Department of Computer Science, Rivers State University, Nigeria. He is an astute researcher who has published numerous works in world journals.