JIRBDAI
Journal of Institutional Research, Big Data Analytics and Innovation

An Enhanced Cloud Security Using Advance Encryption Standard Rail-Fence & Diminished Radix Complement Algorithm for Text Encryption

Seriki Aliu Adebayo[1], Gbolagade kazeem Alagbe[2], Asaju-Gbolagade Ayishat Wuraola[2], Ronke Seyi Babatunde[3], Saka Kayode Kamil[3].

[1]Department of Cyber-Security, Igbinedion University, Okada, Edo State, NigeriaTechnology
[2]Department of Computer Science, Kwara State University, Malete, Nigeria
[2]Department of Computer Science, University of Ilorin, Kwara State, Nigeria
[3]Department of Computer Science, Kwara State University, Malete, Nigeria
[3]Department of Cyber Security, Al-Hikmah University, Ilorin, Nigeria
Corresponding Author: aliyuadebayo7@gmail.com, seriki.aliu@iuokada.com

ABSTRACT A crucial component of cloud computing is cloud security due to the various dangers that arise from cloud environments. Experts in cloud computing and Information Technology (IT) have reported in previous studies that cloud security is a prevalent concern. A few instances of cloud security concerns include data breaches, unauthorized access, and data loss due to system failures or transport. As a result, this study aims to develop an Enhance Cloud Security using Advance Encryption Standard Rail-Fence (AES RFA) and Diminished Radix Complement Algorithm (DRCA) for text encryption for 128, 192 & 256 key bits. In this study, shift row technique was replaced by the Rail-Fence Algorithm (RFA), the Symmetric Algorithm (SA) was introduced, and Bit-wise Transposition Algorithm (BTA) and the Diminish Radix Complement Algorithms (DRCA) were employed in place of the mix column operations. Result showed better computational time of 0.3459sec, 0.3553sec, 0.3659sec was achieved for 128, 192, and 256 Bits respectively. The study concluded that an enhanced cloud security was achieved by using AES RFA and DRCA.

KEYWORDS: Advance Encryption Standard, Bitwise Transposition Algorithm, Diminished Radix Complement Algorithm, Information Technology, Rail-Fence Algorithm, Symmetric Algorithm.

I. INTRODUCTION

Global interest in cloud computing is rising these days, which has encouraged many businesses to try integrating cloud technologies into their operational procedures. Among the many features that make up cloud technology are distributed computing, grid computing, cloud services, storage, and cloud security. Research has received constant interest worldwide ever since the concept of cloud computing was proposed. The various threats that arise from cloud environments make cloud security a crucial component of cloud computing. 96% of cloud users are worried about security in the public cloud, according to Holger (2024) presents few examples of cloud security concerns such as data breaches, unauthorized access, and data loss due to system failures (Chauhan & Shiaeles, 2023). Cloud computing has numerous potentials for businesses, allowing their clients to utilize and access computer services on a "pay-as-you-go" basis. Consumers burdened with batch processing and Web application obligations investigated the cloud computing model as a productive substitute for purchasing and operating private data centers. According to the US National Institute of Standards and Technology (2020) cloud computing is a model that makes it easy to access an infinite pool of shared resources, including servers, storage, applications, software and hardware services. These resources can be quickly made available to clients via the internet upon request, and they can be automatically reviewed upward and downward in response to client demand.

Gartner estimated that by 2026, 10% of all enterprise IT security capabilities with a particular emphasis on web security, messaging, and remote vulnerability assessment will be provided via cloud computing. As technology that support cloud computing improve, other areas of study will be data-loss prevention, encryption, and authentication (Gavaskar, Ragupathy, Ravivarma, and Priyadharshan, 2022). Cloud computing provides

infrastructure, applications, and online data storage. Cloud computing solves the problem of platform reliance. According to Zinabu and Asfera (2022) there are five key components of cloud computing; Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), broad network access, resource pooling, rapid elasticity, and measured service; private, public, community, and hybrid clouds; and Software as a Service (SaaS). A significant amount of study has been devoted to improving methods for cloud data security and efficiency. However, because of the delayed and inadequate security, it was noted that not many research has provided cloud data transfer. The replacement of shift-row operations with a Rail-Fence Algorithm and Symmetric Technique, and the replacement of mix column operations with a Bit-wise Transposition and Diminish Radix Complement Algorithm, have resulted in numerous unresolved challenges regarding improving the security and efficiency of data transfer in the cloud. In order to improve the security and effectiveness of cloud data, this study used an improved AES algorithm with key bits of 128, 192, and 256 that will be applied to text.

II. RELATED WORKS

Mahrousa, Bitar, and Fareed (2020) and Shahiya, Anhanalakshmi, and Lakshana (2023) confirmed that AES's poor diffusion (mix column operation) and confusion (in byte replacement) contributed to its slow pace. As a result, improved diffusion properties were suggested for extending the traditional AES's cipher round and key generation process. Their study's issue, though, is that the mix-column, sub-byte, and shift row operations of the AES algorithm result in a lengthy calculation time. To withstand crypt-analytic attacks, an encryption method that is both adaptive and dynamic is usually necessary. Zinabu, and Adere (2022) proposed a bit-wise reverse transposition technique in place of the mix column stage in the developed cryptography algorithm, the research established the cutting the number of AES rounds for AES of 128, 192, and 256 key bits to 5,6,7 instead of 10, 12, and 14 accordingly. Yet, the problem deduced from the study is that an attacker can easily decipher the operation of swapping which leads to poor security during the bit-wise reverse transposition operation. Specifically, In AES, there are delays in byte substitution, mix-column operations, and lesser security at the second stage of AES algorithm. This has led to many open issues in enhancing the security and efficiency of data transfer in cloud by replacing shift-row operations with a rail-fence algorithm and symmetric technique, and replacing mix column operations with a bit-wise transposition and Diminish Radix complement Algorithm. Hence, this study aimed to enhance Cloud Security Using AES Rail-Fence and Diminished Radix Complement Algorithm for AES 128, 192, and 256 key bits which will be implemented for text files. The table below show the summary of literature of an enhance AES algorithm. Researchers Gavaskar, Ragupathy, Ravivarma, and Priyadharshan (2022) studied a technique that combined two steps: Hybridize Sub-byte with Shift-row operation. The limitation of the study is that there is a computational delay and poor security. Zinabu and Asferaw (2022) found that among the four encryption and decryption phases, Sub Bytes and Mix Column cause the greatest latency. Bitwise Transposition & Symmetric Algorithm were employed. The shortcoming of the study is inadequate security. Riyaldhia, Rojalia, and Kurniawan (2017) proposed a study which used an Array Shift-row mapping and S-box modification. However, high computational time is the drawback of their study. The table below show the summary of literature of an enhance AES algorithm.

Table 1: Summary of Related Literature on Enhanced AES Algorithm

Author/ Year	Title	Technique Used	Limitation
Tran Thi Luong (2023)	Strengthening AES Security Through Key-Dependent ShiftRow and AddRoundKey Transformations Utilizing Permutation	permutation-based Shift-Row and RoundKey transformations	Poor security is the weakness of this study
Zinabu and Asferaw (2022)	Enhanced Efficiency of Advanced Encryption Standard (EE-AES) Algorithm	Bitwise Transposition & Symmetric Algorithm.	Poor security

Gavaskar, Ragupathy, Ravivarma, and Priyadharshan (2022)	AES Algorithm using Dynamic Shift Rows, Sub Bytes and Mix Column Operations for Systems Security with Optimal Delay	Hybridize Sub-byte with Shift-row operation	Poor security and computational delay
Riyaldhia, Rojalia, and Kurniawan (2017)	Improvement of Advanced Encryption Standard Algorithm with Shift Row and S.Box Modification Mapping in Mix-column	Array Shift-row mapping and S-box modification	High computational time and poor security

III. METHODOLOGY

The traditional AES Algorithm is shown in Figure 1:

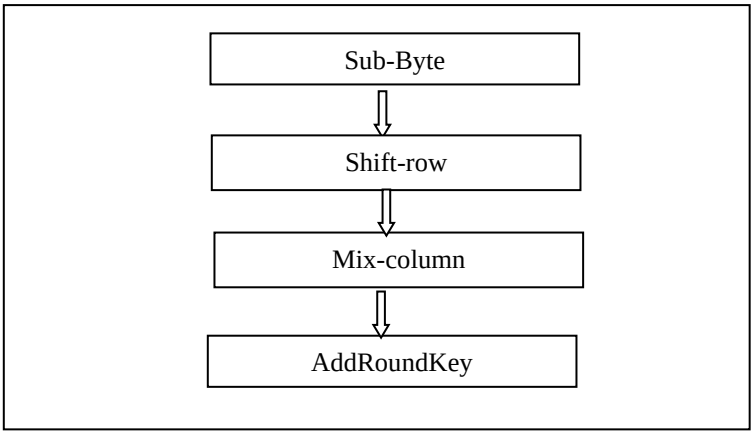


Figure 1: Traditional AES Algorithm

However, due to computational delay in the shiftrow and mix-column operation of the traditional AES, Zinabu and Asferaw (2022) proposed an algorithm which eliminate both mix-column and shiftrow as shown in Figure 2.

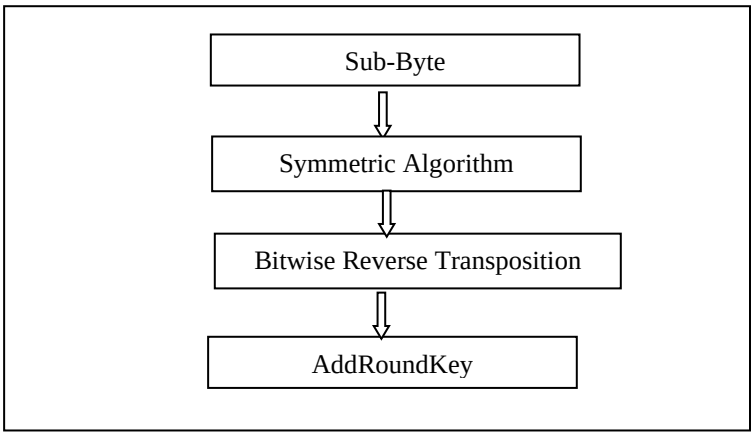


Figure 2: Existing Algorithm (Zinabu & Asferaw, 2022)

The existing algorithm of Zinabu & Asferaw (2022) has a limitation in security level; in order to address that, Rail-fence Algorithm was used with Symmetric Algorithm so as to have strong randomness and Bitwise Transposition with Diminished Radix Complement Algorithm to improve the diffusion. This is shown in Figure 3 where Rail-fence Algorithm and Diminished Radix complement Algorithm have been introduced.

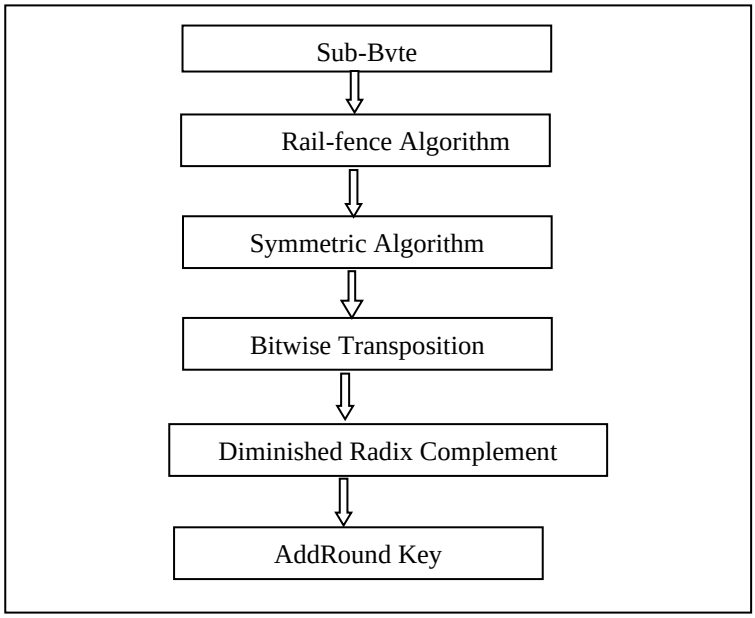


Figure 3: Propose AES-RFA & DRCA Algorithm

To achieve the aim of this study, Figure 4 show the detail steps for the methodology adopted for this study.

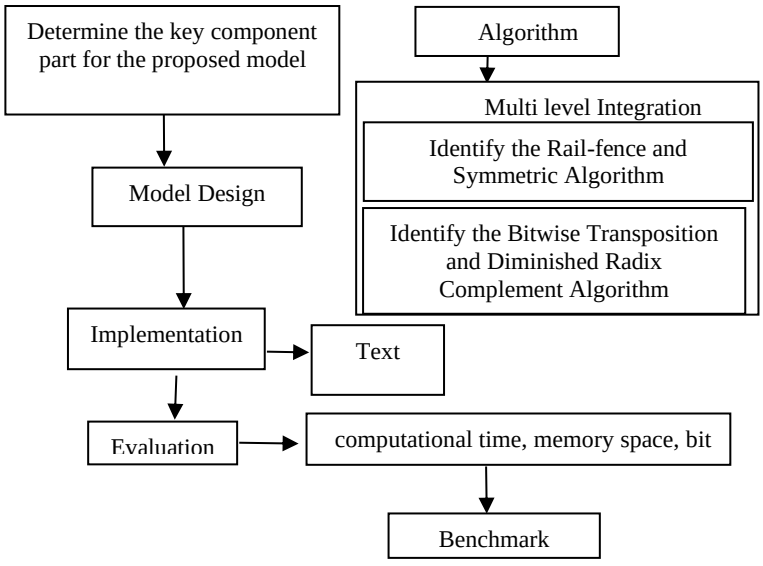


Figure 4: Research Methodology

i. Sub-Byte: every byte in the state is changed to an alternate byte at this stage using a substitution box. The outcome is a non-linear and jumbled set of data. The Sub-Bytes() modification is a non-linear byte replacement that operates independently on each byte of the State (S-box) using a substitution table. Figure 2 displays an S-box. replacement values (in hexadecimal format) for the byte xy, for example:

$$\begin{pmatrix} EA & 04 & 65 & 85 \\ 83 & 45 & 5D & 96 \\ 5C & 33 & 98 & B0 \\ F0 & 2D & AD & C5 \end{pmatrix}$$

the intersection of the row with index 'E' and the column with index 'A' would yield the substitution value if s1,1 {EA}. As a result, s1,1 would have a value of {87} in the S-Box table.

EA	04	65	85
83	45	5D	96
5C	33	98	B0
F0	2D	AD	C5

⇒

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

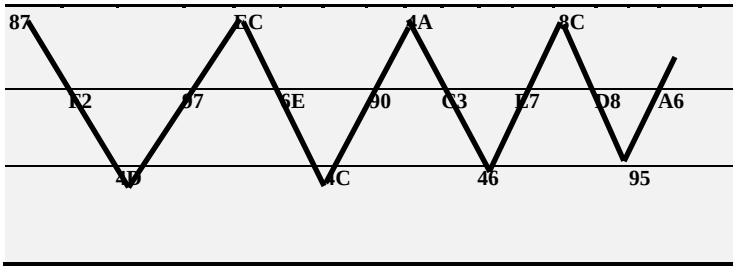
ii. Rail-fence algorithm: This is also called a zig zag algorithm. The algorithm is as follows:

Algorithm for Rail-Fence

(a). The plain-text/ digit is written downwards and diagonally on successive rails of an imaginary fence.

(b). When we reach the bottom rail, we climb upwards moving diagonally, after reaching the top rail, the direction is changed again. The message's alphabets are therefore written in a zigzag pattern.

(c). The individual rows are concatenated to create the cipher-text once each alphabet has been written.



87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

⇒

87	EC	4A	8C
F2	97	6E	90
C3	E7	D8	A6
4D	4C	46	95

ii**i. Symmetric algorithm**: By replacing the third stage, the symmetrical transposition stage, with the Rail- fence technique, the AES method's data encryption security is increased. Here is how the symmetric algorithm works:

Algorithm for symmetric

(a). Swapping non-major diagonal items that are symmetrical around the main diagonal elements in position.

(b). Swapping the major diagonal components that are symmetrical around the non-primary diagonal elements in their positions

87	EC	4A	8C
F2	97	6E	90
C3	E7	D8	A6
4D	4C	46	95

⇒

95	F2	C3	4D
EC	D8	E7	4C
4A	6E	97	46
8C	90	A6	87

iv. **Bitwise Transposition algorithm**: the algorithm for bitwise transposition is as follows:

Algorithm for Bitwise Transposition

(a). First, transfer the components from the first row of the input to the first column of the output. Next, swap bitwise a21 and bitwise a31 in the output.

(b). Moving the components from the input's second row to the output's third column, and then bit-by-bit switching a23 with a33 in the output.
(c). Transferring the items from the third row of the input to the second column in the output, and then bit-by-bit reversing and exchanging rows a22 and a32.
(d). Copying the components from the fourth row of the input to the fourth column of the result, and mixing up bits a24 and a34 in the result.

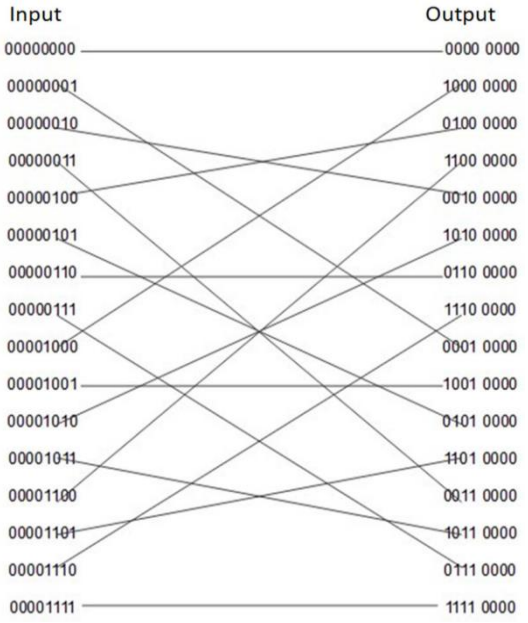
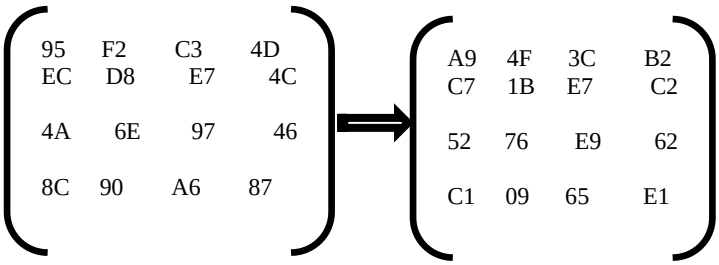


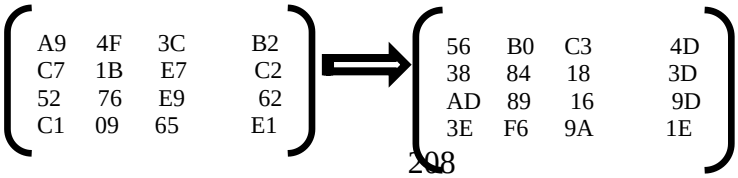
Figure 5: Internal Structure of Bitwise Reverse Transposition (Zinabu and Asferaw, 2022)



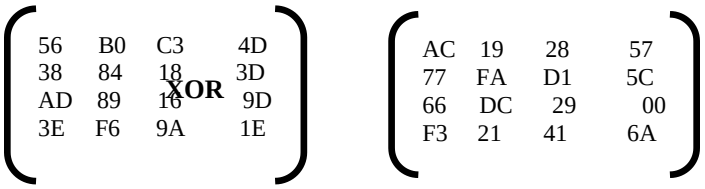
v. Diminished Radix Complement Algorithm: This method cannot be compared to either the original AES technology or the improved AES based on the Bitwise transposition algorithm. When compared to the existing AES technique, it shows an improved security operation. The digits of the matrix are all transformed into binary and toggled.

$\overline{A9}$ = 1010 1001 is toggled and we have
$\overline{A9}$ = 0101 0110 => 56
$\overline{4F}$ = 0100 1111
4F=10110000=>B0

The matrix below shows how almost all of the input data significantly increases the result's confusion. We now have:



vi. Add Round-key:Bitwise XOR is used in this last stage of every round to add a round key (which is derived from the main key) to the state. By taking this step, it is ensured that the encryption key is used in each cycle.



56 ⊕ AC => 56= 0 1 0 1 0 1 1 0

=>AC=1 0 1 0 1 1 0 0 ⊕

1 1 1 1 1 0 1 0 → FA

B0 ⊕ AC => B0= 1 0 1 1 0 0 0 0

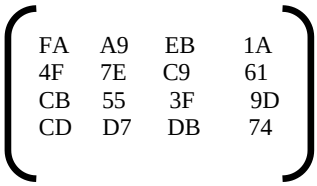
=>AC=1 0 1 0 1 1 0 0 ⊕

1 0 1 0 1 0 0 1 → A9

C3 ⊕ 28 => C3= 1 1 0 0 0 0 1 1

=>28=0 0 1 0 1 0 0 0 ⊕

1 1 1 0 1 0 1 1 → EB



IV. RESULTS AND DISCUSSION

The proposed algorithm was used to address data breaches, unauthorized access, and data loss due to system failures or transport in cloud (google drive, salesforce). To implement AES-RFA & DRCA in cloud security, the AES algorithm was improved by introducing RFA to replace shift row operation and DRCA was introduce instead of mix column. The proposed algorithm minimized the brute force attack (trying different key combination to decipher message) where by Rail-fence and Symmetric Algorithm was used to improve the randomness of the AES so as to make it difficult for an attacker to decipher the encrypted message. The work computes AES RFA and DRCA for 128, 192, and 256 Bits respectively. The enhance Cloud Security was implemented with a model with a Graphical User Interface (GUI) to help in the encrypting and decryption stages as shown in Figure 6:

Figure 6: GUI of AES RFA & DRCA

Figure 6 shows the sections: select AES key bit, enter plaintext text (right-side), encrypted text (leftt-side). The result obtainable in Table 1 shows the performance of the AES RFA & DRCA computational time of 128, 192, and 256 Bits. The develop technique is subject to some tests to affirm its enhancement in terms of time taken and memory space. In addition, the computational time of the developed technique is recorded and compared with the existing system. The proposed algorithm was tested for 128, 192, and 256 bit keys respectively as shown in the table below

Table 2: Encryption, Decryption time. Memory space for AES RFA & DRCA Bits

AES RFA &DRCA Key Bits	Encryption Time	Decryption Time (sec)	Memory Space
128	0.3459	0.3458	81 bytes
192	0.3553	0.3557	113 bytes
256	0.3659	0.3663	145 bytes

Table 2 display the computational time of the propose Algorithm compare with the existing studies

Table 3: Comparison of the Propose Technique Encryption Time with Existing Studies

Author (Years)	Title	Encryption Time (sec)	Decryption Time (sec)
Propose Algorithm (2024)	An Enhanced Cloud Security Using Advance Encryption Standard Rail-Fence & Diminished Radix Complement Algorithm for Text Encryption	0.3459	0.3458
Aditya and Lavanya (2023)	A decentralize storage system for 3D Medical Data with Dynamic AES and AES-GCM Encryption	4.9	2.32
Zinabu and Asferaw (2022)	Enhanced Efficiency of Advanced Encryption Standard (EE-AES) Algorithm	0.3374	4.264

Riyaldhia, Rojalia, and Kurniawan (2017)	Improvement of Advanced Encryption Standard Algorithm with Shift Row and S.Box Modification Mapping in Mix-column	3.56	3.81

The graph below shows the proposed Algorithm with the existing system:

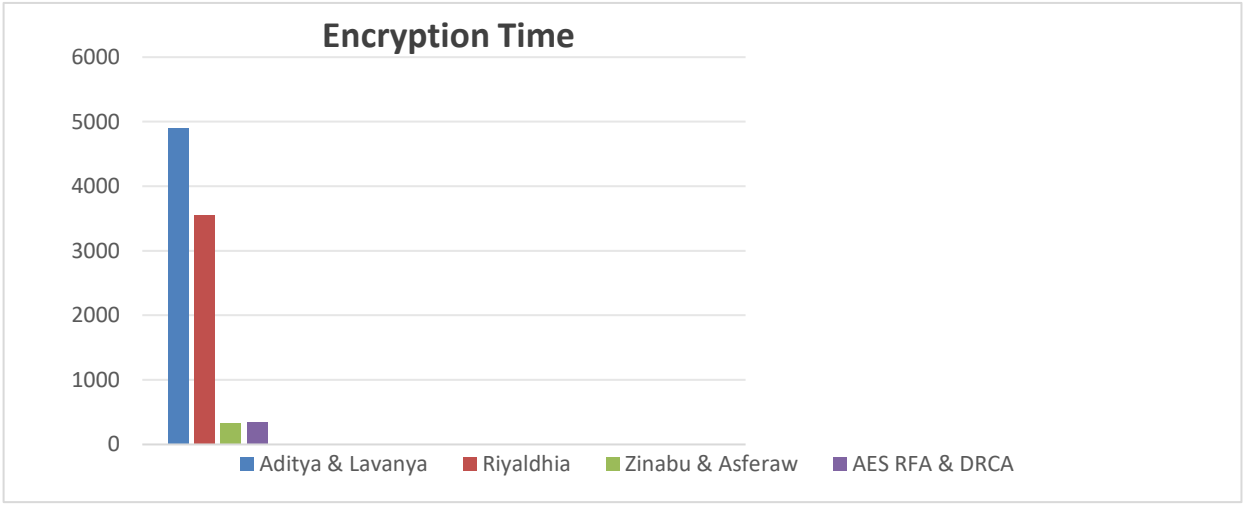


Figure 7: Comparison of the Encryption Time Bar Graph with Existing System

V. CONCLUSION

AES, RFA and DRCA were employed in this work to improve cloud security. In order to improve cloud security, we investigated the methods of RFA in conjunction with SA and DRCA in conjunction with BTA. Strong randomness is provided by the integration of RFA, which is followed by the incorporation of SA, DRCA, and BTA. This technique increases the security of data in the cloud and has been shown to be a successful strategy for boosting the effectiveness and security of the cryptography system. The findings of this study demonstrated that the multi-level approach addresses the shortcomings of both the current system and the conventional AES by providing notable enhancements in differentiating between secure and efficient data in the cloud. The suggested model is a workable solution for practical applications since it combines the advantages of RFA and DRCA to guarantee computational efficiency while simultaneously enhancing security.

REFERENCES

[1]. Milan Chauhan, and Stavros Shiaeles (2023). An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions, Network 2023, 3, 422–450. *Network* 2023, 3, 422–450. https://doi.org/10.3390/network3030018.

[2]. Gavaskar K, Ragupathy U S, Ravivarma G, and Priyadharshan P S (2022). AES Algorithm using Dynamic Shift Rows, Sub Bytes and Mix Column Operations for Systems Security with Optimal Delay. *Research square.*

[3]. G Aditya and V Lavanya (2023). A decentralize storage system for 3D Medical Data with Dynamic AES and AES-GCM Encryption. *Recent Developments in Electronics and Communication Systems*.

[4]. Holger Schulze (2024) Cloud Security Report

[5]. Milan Chauhan, and Stavros Shiaeles (2023). AnAnalysis of Cloud Security Frameworks, Problems and Proposed Solutions, *Network 2023*, 3, 422–450. Network 2023,3,422–450.

[6]. Nahom Gebeyehu Zinabu, and Ketema Adere (2022). Enhanced Image Cipher and Decipher Speed of Advanced Encryption Standard Algorithms for EmbeddedDevices.https://*www.researchgate.net/publication*/379121266.

[7]. Nahom Gebeyehu Zinabu, and Samuel Asferaw (2022). Enhanced Efficiency of Advanced Encryption Standard (EE-AES) Algorithm. *American Journal of Engineering and Technology Management*, 2022; 7(3): 59-65.

[8]. Rizky Riyaldhia, Rojalia, and Aditya Kurniawan (2017). Improvement of Advanced Encryption Standard Algorithm with Shift Row and S.Box Modification Mapping in Mix-column, *2nd International Conference on Computer Science and Computational Intelligence 2017* (ICCSCI 2017), 13-14 October 2017, Bali, Indonesia.

[9]. Sanhanalakshmi Mahalingam, Lakshana Kahirvel, and Shahiya G. Maheswari (2023). Enhanced AES-256 cipher round algorithm for IoT applications. *The Scientifc Temper* (2023) Vol. 14 (1): 184-190.

[10]. Tran Thi Luong (2023). Strengthening AES Security Through Key-Dependent ShiftRow and AddRoundKey Transformations Utilizing Permutation, *International Journal of Advanced Computer Science and Applications* (IJACSA), Vol. 14, No. 11, 2023.

[11]. Zakria Mahrousa, Ahmad Bitar, and Yahia Fareed (2020). A Novel Method to Increase Diffusion and Confusion in AES Algorithm, *International Journal of Computer Applications* (0975 – 8887),Volume 177 – No. 36, February 2020.