ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

AES SECURITY IMPROVEMENT BY UTILIZING NEW KEY-DEPENDENT XOR TABLE

E. MOUNIKA REDDY [1], KANAPARTHI NIKHIL[2], BUDDE NIKHILESH RISHIDHAR [3], NALLAPU AKSHAY VARMA [4], ATHKURI RAMESH [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— Increasing the security of block ciphers is a topic of great interest today, and thus there is a variety of work to enhance the strength of such ciphers. There are also many studies focusing on the Advanced Encryption Standard (AES), presenting methods of making block ciphers dynamic to improve their security. Animating methods can perform block cipher transformations such as substitution or permutation, or both. In this article, we propose an algorithm to create new, key-dependent XOR tables from an initial secret key. At the same time, we prove that in the cipher text the new XOR operation can preserve the independent, co-probability distribution of the random key. We then apply these new XOR tables to make AES dynamic at the Addroundkey transformation. We created a considerable number of XOR tables, about (16!) 2 tables. With such a vast number of key-dependent dynamic XOR tables, cryptanalysts will have great difficulty finding the actual XOR table used in the modified AES block cipher. Therefore, with our new XOR tables, AES will be significantly enhanced.

Index Terms – AES, Key-Dependent XOR Table, Symmetric Encryption, Cryptography, Data Security, Block Cipher, Secure Communication, Information Security, Cybersecurity, Encryption.

I. INTRODUCTION

For global partnership scientific collaborations and review system should

facilitate data sharing, confidential peer review process to critically evaluate the outcome, transparent and audit-able process with policies beneficial to the partnership. These key aspects are shown in Figure1. Peer review is the key to the growth of scientific knowledge which validates the credibility and legitimacy of the science. Though being claimed as instrumental for raising quality of publications, it still lacks transparency. With the soaring advancement in IT, researchers have proposed integration of scientific publishing system with blockchain for its inherent feature of immutability. Patent heathcare data review comments research datasets are proposed to integrate with blockchain for its immutability feature. With the improvement in the traceability of review process, the existing work does not address the implementation of confidentiality in the review process or research data sharing. Reviewers breach of confidentiality causes year long hardship of researchers down the drain. Fake reviews, lack of verifiability, vulnerability to manipulation, privacy concerns are some of the keys issues of existing review management system. Thus, review process mandates confidentiality in manuscript submission to reviewers and to the review comments. On the same grounds sharing of confidential research data need to be carefully handled to avoid breach of HIPAA(Health Insurance Portability and Accountability Act)Act or jeopardize participants identity. For audit-ability of records blockchain can be proposed to use which ensures record retention even after the destruction of smart contracts. Without the exchange of research material, the collected data gets stagnated and eventually will face lock-in effect. Moreover data owners may have diverse expectations regarding their data, including preferences for affiliations from institutions with which they have signed memoranda of understanding (MoUs) or collaborative plans for specific time frames. These expectations may vary based on the geographical origins of the data owners, which aligns with findings of Dutra et al.where only one third of authors sent the requested data for systematic literature work. To accommodate differences in opinion, a Zero Trust Architecture is inculcated in data access scenario. This architecture evaluates if the researchers are capable enough to handle the set expectations. Thus the work concentrates on evaluating data access requests and secure data sharing, essential for scientific reproducibility and verifiability. Thus effective monitoring of the access activities of data or resources under authorized legitimate conditions can be

implemented by access control mechanism. It is urgent to strengthen the peer review confidentiality and privacy of research data. The work proposes to address confidentiality in the blockchain based review process, sensitive data access request and sharing for scientific collaborations. The work enforces access control mechanism using blockchain based smart contracts since it involves collaboration between untrusted parties. Restricting unauthorized users from accessing the confidential data is ensured using AES encryption symmetric key generated using HKDF algorithms and incorporating Lagrange Interpolation for consensus between multi-partied data ownership, thus avoiding cyber incident on data silos. Summarizing the contributions of the work are as follows: 1) Addressing confidentiality in review process to ensure secure and coordinated handling of unpublished manuscript between author, editor and assigned reviewers. 2) Proposing Zero trust (ZT) architecture for processing confidential data access request ensuring accountability of context based opinions between various data owners in varying hierarchy. 3) To ensure confidential data sharing after ZT acceptance. 4) To incorporate author feedback on review comments adding value added recommendation to editor for selection of future reviewers.

II. RELATED WORK

A. Combined interleaved pattern to improve confusion-diffusion image encryption based on hyperchaotic system

The quality of encryption is dependent on the complexity of the confusion-diffusion pattern and the quality of the keystream employed. To enhance complexity and randomness, this study proposes a combination of multiple interleaved patterns, including Zigzag, Hilbert, and Morton patterns to complicate the confusion-diffusion. The keystream is generated from the improved logistic map and the 6D hyperchaotic map, which complement each other due to their sensitivity to initial conditions and control parameters. This produces highly random and nonlinear keystreams, making them difficult to predict. The encryption process consists of four phases, alternating between diffusion and confusion. Furthermore, SHA-512 is used to enhance key space and sensitivity. Based on the test results, the proposed encryption technique can withstand various attacks, such as statistics, differential,

brute force, and NIST randomness tests, as well as data loss and noise attacks. Most of the results are better than previous studies.

B. *Building the dynamic diffusion layer for SPN block ciphers based on direct exponent and scalar multiplication.*

Maximum Distance Separable (MDS) matrices have been applied not only in coding theory but also in the design of block ciphers and hash functions. In this paper, we propose algorithms for building a dynamic diffusion layer for SPN block ciphers based on the direct exponent and scalar multiplication. The proposed dynamic algorithms contribute to improving the security of SPN block ciphers against strong attacks on block ciphers such as linear attacks, differential attacks. In cryptography, confusion and diffusion are two indispensable properties of a secure cipher. The simplest way to achieve these properties is a substitution-permutation network. This network takes as input a plaintext block and a secret key and applies many transformation "rounds" or "layers" of substitution boxes (S-boxes) and permutation boxes (P-boxes) to create cipher text block. MDS matrices play a very important role in block cipher design, especially substitution permutation network (SPN). Therefore, they have been used for many ciphers today. To improve the security of block ciphers, there are some methods for making dynamically these ciphers such as make dynamically at the substitution layer, at the diffusion layer or both. For the method making dynamically at diffusion layer, there are some works in the literature about this direction. In and the authors generated key-dependent MDS matrices for each round of encryption to build a key dependent diffusion layer. In permutation and scalar multiplication of the rows of the matrix are used, where scalar multiplication and permutation are generated from a secret key and a random bit generator function. In dynamic MDS matrices are also generated using scalar multiplication for each round, where a secret key and a random bit generator are generated by the scalar multiplication. In a dynamic block cipher was proposed. This cipher is made dynamically at both substitution and permutation layers by a bank of substitution boxes and key dependent MDS matrices.

C. *Fast computation of direct exponentiation to speed up implementation of dynamic block ciphers*

MDS (maximum distance separable) matrices are ones that come from MDS codes that have been studied for a long time in error correcting code theory and have many applications in block ciphers. To improve the

security of block ciphers, dynamic block ciphers can be created. Using MDS matrix transformations is a method used to make block ciphers dynamic. Direct exponentiation is a transformation that can be used to generate dynamic MDS matrices to create a dynamic diffusion layer of the block ciphers. However, for cryptographic algorithms that use an MDS matrix as a component of them, the implementation of matrix multiplication is quite expensive, especially when the matrix has a large size. In this paper, the mathematical basis for quick calculation of direct exponentiation of an MDS matrix will be presented. On that basis, it is to suggest how to apply that fast calculation to dynamic algorithms using the direct exponentiation. This result is very meaningful in software implementation for MDS matrices, especially when implementing dynamic block ciphers to increase execution speed.

III. PROPOSED METHODOLOGY

The proposed system introduces a novel approach by integrating dynamic XOR tables that depend on the secret key into the AES algorithm.

The dynamic and key-dependent nature of the XOR tables adds a layer of complexity that can enhance security against certain types of attacks.

This dynamic feature aims to complicate the encryption by making the XOR operation dependent on the key, thereby increasing resistance to cryptanalysis.

This dynamic approach introduces significant variability into the encryption process, making the XOR operation unpredictable and less susceptible to attacks that exploit static patterns.

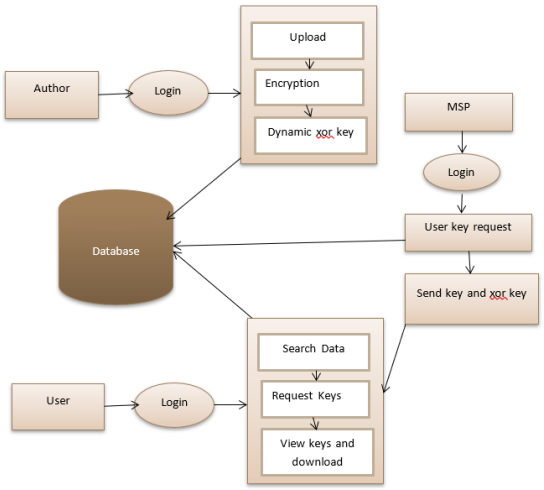
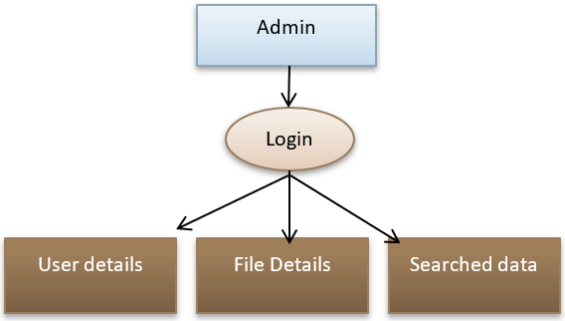


Fig. 1: System Overview

1. Admin

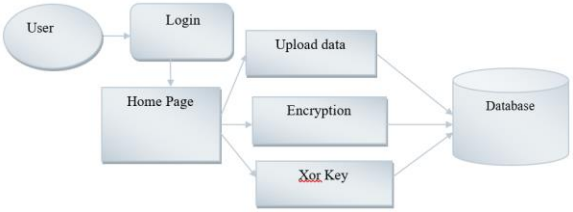
This is the Second module in our project is Admin. Here admin will login with his password and Id who has created by the bc operator. After admin login directely will navigate into admin home page. The purpose of an administrator is to oversee and manage the operations and functionality of an organization, system, or project. Administrators are responsible for

coordinating tasks, enforcing policies, and ensuring that processes run smoothly and efficiently.



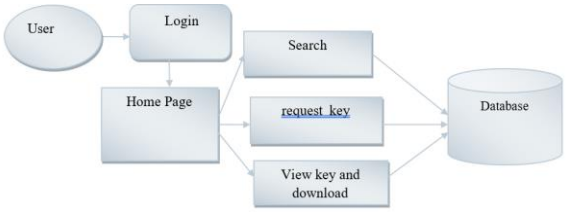
2. Owner

This is the Third module in our project is Owner. Here User will login with user email and password. After login it will directly navigate home page there user can upload and search data, then it will show related data. If he/her want to access data he should take request from author who uploaded data.



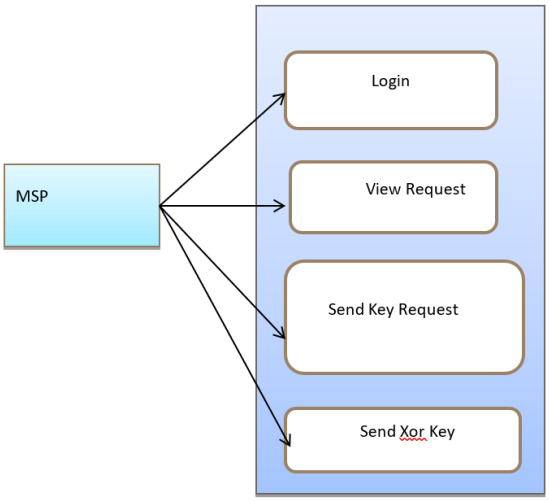
3. Search

This is the Fourth module in our project is Search. Here User will login with user email and password. After login it will directly navigate home page there user can search his data, then it will show related data. If he/her want to access data he should take request from author.



4. MSP

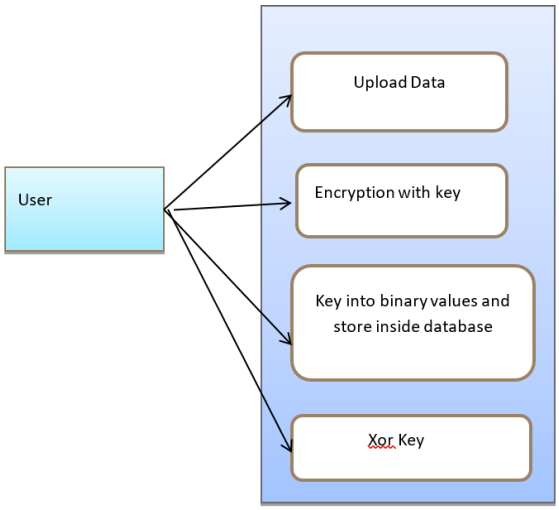
This is the Fifth module in our project is Msp. Here msp will login with user email and password. After login it will directly navigate home page here msp acts as third part where it shares xor dynamic keys to user.



5. Encryption

Encryption is a process used to secure information by transforming it into a format that is unreadable to anyone who does not have the appropriate decryption key. Essentially, encryption converts plaintext (readable data) into ciphertext (encoded data) using a specific algorithm and key. This transformation ensures that even if the data is intercepted or accessed without authorization, it remains protected and

inaccessible without the correct decryption mechanism.



IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrated that the introduction of the key-dependent XOR table increased the randomness of the encryption process, producing highly secure ciphertext while maintaining efficient encryption and decryption performance. The enhanced AES algorithm successfully encrypted data with minimal computational overhead compared to the conventional AES implementation.

The analysis showed that the proposed approach exhibited high key sensitivity, strong avalanche effect, and improved resistance against brute-force, differential, and statistical attacks.

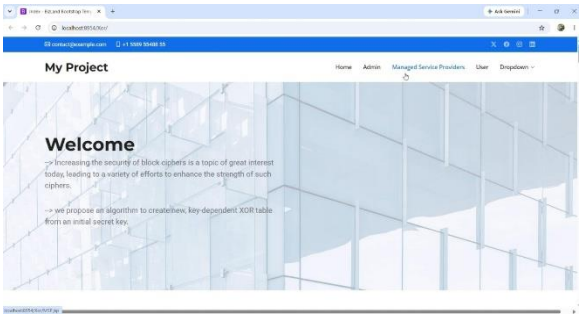


Fig. 2: Home Page

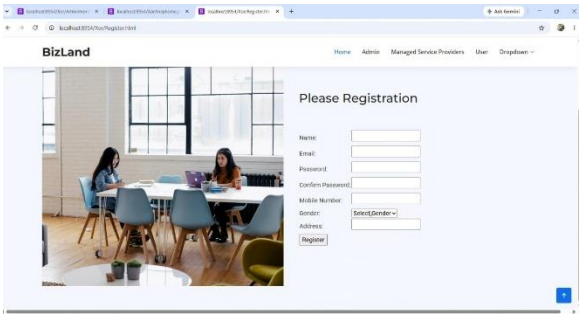


Fig. 3: Register

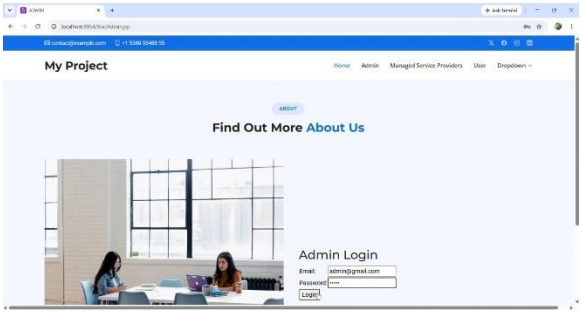


Fig. 4: Admin Login

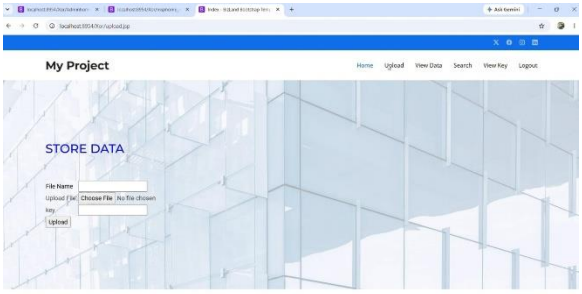


Fig. 5: Store Data

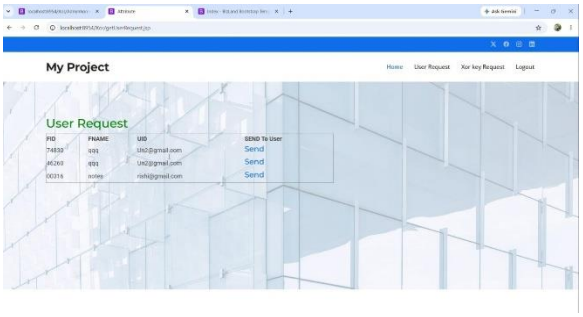


Fig. 6: User Request

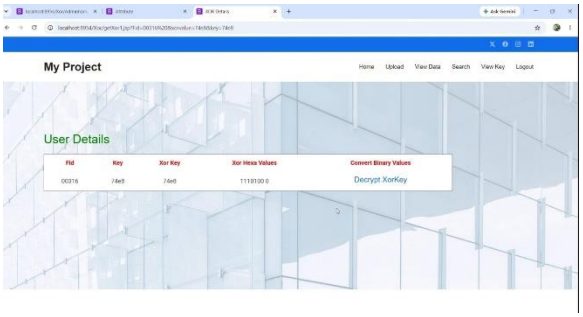


Fig. 7: User Details

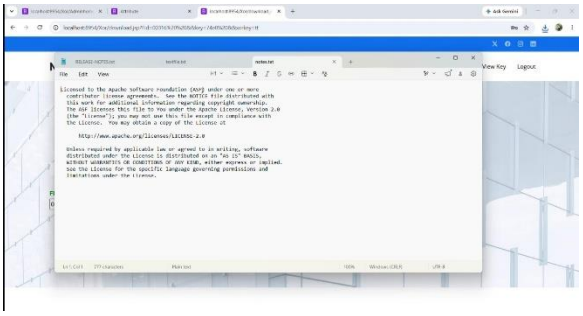


Fig. 8: Decrypted Data

V. CONCLUSION

In an effort to enhance the strength of SPN block ciphers, including the AES block cipher, dynamic approaches may target individual parts of the ciphers, such as the diffusion layer transformation, substitution transformation, or both. This manuscript introduces a technique for rendering AES dynamic at the key addition transformation with key-dependent XOR tables. Within this study, we outline the requisite characteristics of an XOR table and we prove the correctness of the new XOR table generated by our method. Notably, the revised XOR operation can maintain the uniform probability and independent distribution of the random key in the ciphertext. We analyze the security of the altered AES block cipher, and the number of key-dependent XOR tables that can be created through our approach is equivalent to (16!) 2 . With such an extensive array of new XOR tables, cryptanalysts will face significant challenges in ascertaining the specific XOR table employed in the altered AES block cipher.

REFERENCES

[1] C. E. Shannon, ‘‘Communication theory of secrecy systems,’’ Bell Syst. Tech. J., vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] P. L. Andono and D. R. I. M. Setiadi, ‘‘Improved pixel and bit confusion-diffusion based on mixed chaos and hash operation for image encryption,’’ IEEE Access, vol. 10, pp. 115143–115156, 2022, doi: 10.1109/ACCESS.2022.3218886.

[3] E. Winarno, K. Nugroho, P. W. Adi, and D. R. I. M. Setiadi, ‘‘Combined interleaved pattern to improve confusion-diffusion image encryption based on hyperchaotic system,’’ IEEE Access, vol. 11, pp. 69005–69021, 2023, doi: 10.1109/ACCESS.2023.3285481.

[4] S. Beg, N. Ahmad, A. Anjum, M. Ahmad, A. Khan, F. Baig, and A. Khan, ‘‘S-box design based on optimize LFT parameter selection: A practical approach in recommendation system domain,’’ Multimedia Tools Appl., vol. 79, nos. 17–18, pp. 11667–11684, May 2020, doi: 10.1007/s11042- 019-08464-6.

[5] S. Mister and C. Adams, ‘‘Practical S-box design,’’ in Proc. Workshop Sel. Areas Cryptography (SAC), vol. 96, Aug. 1996, pp. 61–76.

[6] A. M. Youssef and S. E. Tavares, ‘‘Resistance of balanced S-boxes to linear and differential cryptanalysis,’’ Inf. Process. Lett., vol. 56, no. 5, pp. 249–252, Dec. 1995, doi: 10.1016/0020-0190(95)00156-6.

AUTHORS Profile

Mrs. E. MOUNIKA REDDY has received her B.Tech from JNTUH, Hyderabad in 2015, M.Tech degree in Computer science from JNTUH, Hyderabad in 2017. She is dedicated to teaching field from the last 8 years. At present she is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.

Mr. KANAPARTHI NIKHIL pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. BUDDE NIKHILESH RISHIDHAR pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. NALLAPU AKSHAY VARMA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. ATHKURI RAMESH pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.