IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 12, Issue 3, May-June 2025

Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203035

Boosting AES Security: A Key-Dependent XOR Table Approach for Improved Encryption

Ramavath Ankitha, Ravula Nithin Yadav, Varun Teja, Dr.Ch. Ravindra

Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad, India

Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad, India

Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad, India

Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad, India

ABSTRACT: Enhancing the security of block ciphers is a critical area of research, with many approaches aimed at strengthening their resistance to cryptanalysis. One such approach focuses on adding dynamism to the Advanced Encryption Standard (AES), improving its robustness. This paper introduces an innovative method for dynamically generating key-dependent XOR tables, which are used to modify the AES cipher. The algorithm we propose creates new XOR tables from an initial secret key, ensuring that the transformed ciphertext maintains the independence and coprobability distribution of the original key. We apply these dynamic XOR tables to the AddRoundKey transformation within AES, significantly increasing the number of possible XOR tables—approximately (16!)^2 tables—making it much more challenging for attackers to identify the correct table used in the encryption process. This dynamic modification enhances AES's security by greatly complicating cryptanalysis, thereby providing a more secure encryption scheme.

I. INTRODUCTION

1. GENERAL

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

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203035

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. SCOPE OF THE PROJECT

The scope of this project encompasses several key areas focused on enhancing the security of the AES (Advanced Encryption Standard) block cipher through a novel approach involving dynamic XOR tables. Our research introduces a dynamic AES variant by incorporating XOR tables that are dependent on the encryption key, aiming to improve the cipher's resilience against various cryptanalytic attacks. The dynamic XOR tables are applied to the AES key-addition transformation, creating a modified AES algorithm. A comprehensive security analysis is conducted to evaluate the robustness of this modified AES against potential attacks.

III. OBJECTIVE

The primary objective of this project is to enhance the security of the Advanced Encryption Standard (AES) block cipher by introducing a novel approach that utilizes dynamic XOR tables dependent on the encryption key. This approach aims to fortify AES against various cryptanalytic attacks by incorporating key-dependent transformations that complicate the identification of the XOR tables used. We seek to demonstrate that our method improves the cipher's resilience by generating a larger number of dynamic XOR tables, which increases the difficulty for attackers to predict or exploit the encryption process.

IV. PROBLEM STATEMENT

Despite its widespread adoption and reputation as one of the most robust encryption algorithms available today, AES (Advanced Encryption Standard) is not without its vulnerabilities. As cryptographic techniques evolve and computational power increases, concerns about AES's security have emerged. The algorithm's relatively straightforward mathematical structure might be susceptible to future attacks, such as algebraic attacks. Additionally, the persistent threat of linear and differential attacks poses a significant risk, particularly if an adversary can amass large volumes of plaintext-ciphertext pairs. The advancement of supercomputing technology raises the specter of feasible brute-force attacks on AES keys. Moreover, the advent of quantum computing introduces new challenges; for instance, Grover's algorithm could potentially reduce the effective key length, demanding longer keys to maintain equivalent security. Therefore, there is a pressing need to address these vulnerabilities and strengthen AES against emerging threats.

V. EXISTING SYSTEM

- AES can be considered one of the strongest and most widely used encryption algorithms in the world today, extensively applied in various security applications.
- However, AES itself has inherent vulnerabilities that cryptanalysts could potentially exploit to attack this block cipher. Some cryptographic experts express concerns about AES's security.
- A well-established symmetric encryption standard with fixed transformations and wellstudied security properties.
- AES operates on 128-bit blocks of data and employs a fixed series of transformations including SubBytes, ShiftRows, MixColumns, and AddRoundKey, using static keydependent round keys to secure data.

VI. EXISTING SYSTEM DISADVANTAGES

- While AES is robust against many forms of attack.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203035

- AES uses fixed parameters throughout its encryption process.
- It might not be optimal for scenarios where additional layers of security or adaptability to different attack vectors are desired.

VII. LITERATURE SURVEY

Title: Combined interleaved pattern to improve confusion-diffusion image encryption based on hyperchaotic system.
Author: E. Winarno, K. Nugroho, P. W. Adi, and D. R. I. M. Setiadi.
Year: 2023.

Description:
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.

VIII. PROPOSED SYSTEM

- 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.

IX. PROPOSED SYSTEM ADVANTAGES

- Increased Security.
- As the XOR tables are generated based on the key, the encryption scheme can adapt to different keys and potentially different attack strategies, providing a more robust defense mechanism.

X. APPLICATION

GENERAL

Finally, a rank of data containing the filtered data with correlation value is given as the data feed.

FUTURE ENHANCEMENT

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. Lastly, both the AES block cipher and dynamic AES block cipher were assessed for randomness utilizing NIST statistical criteria. The results of the experiment indicate that both the altered AES and AES algorithms exhibit randomness after three rounds with a random key and input data sets Rot, HW, LW, Av1, and after four rounds with a zero key and input data sets Rot, HW, LW, Av1, both exhibit randomness. Therefore, the method proposed has the ability to generate a dynamic AES block cipher that strengthens the strength of AES against various powerful attacks targeting block ciphers. In our upcoming research, we plan to integrate dynamic techniques into the substitution, key addition, and diffusion layers to enhance the security of SPN block ciphers even further. Simultaneously making multiple components of the block cipher dynamic will make it more

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203035

challenging for attackers to carry out attacks. We will also invest more time and effort in researching specific attacks, especially conducting linear and differential attacks against
the proposed dynamic block ciphers

IX. 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 keydependent 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. 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: 10.1016/00200190(95)00156-6.
7. W. Koo, H. S. Jang, and J. H. Song, "On constructing of a 32 × 32 binary matrix as a diffusion layer for a 256-bit block cipher," in Proc. Int. Conf. Inf. Secur. Cryptol., Germany. Berlin, Springer, 2006, pp. 51–64.
8. M. Kumar, P. Yadav, S. Pal, and A. Panigrahi, "Secure and efficient diffusion layers for block ciphers," J. Appl. Comput. Sci. Math., vol. 11, no. 2, pp. 15–20, 2017.
9. H. N. Noura and A. Chehab, "Efficient binary diffusion matrix structures for dynamic keydependent cryptographic algorithms," J. Inf. Secur. Appl., vol. 68, Aug. 2022, Art. no. 103264.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975

Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com