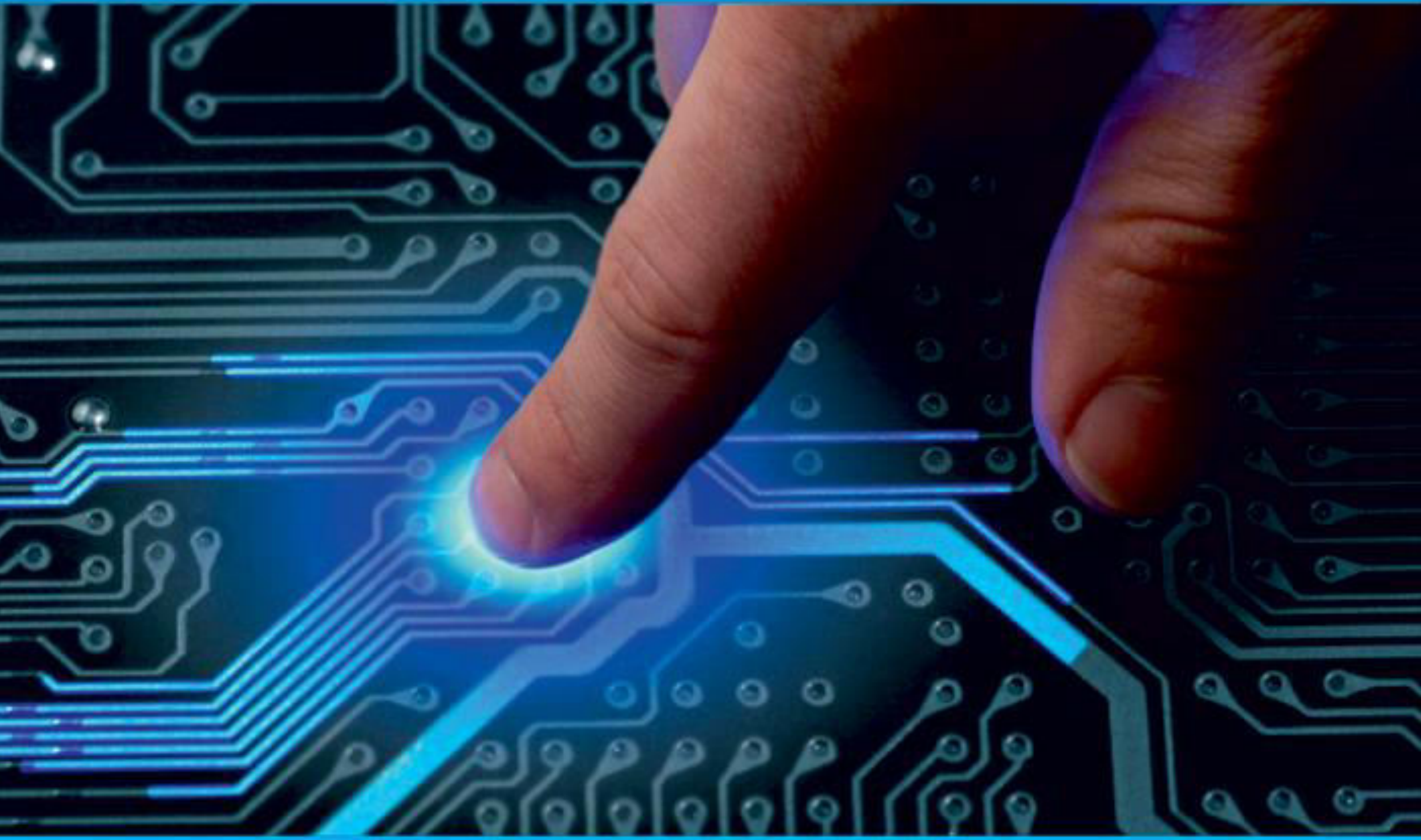
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203056 |

Enhancing Data Protection through Advanced Encryption or Improving Data Security with Advanced Encryption

Mataz Ali N[1] , Haripriya V[2]

PG Student, School of CS & IT Jain (Deemed-to-be-University), Bengaluru, India[1]

Assistant Professor, Department of School CS&IT, Jain (Deemed-to-be-University), Bengaluru, India[2]

ABSTRACT: The protection of information content is becoming a key concern with the recent exponential growth of digital data interchange over computer networks. Numerous security vulnerabilities can readily jeopardize the information sent over a network. An enhanced modification for the Advanced Encryption Standard (AES) algorithm is proposed and implemented using an additional key that generated using a linear feedback shift register (LFSR), which provides an efficient technique to pseudo random number generation and also reduces the number of rounds. Cryptography plays a crucial role in ensuring the security of digital data transmission over these unsafe networks. When compared to the original AES algorithm result, the suggested technique produces the expected results for several data types, including text, images, It is more important than ever to strengthen data protection procedures in an era of rising cyber dangers and growing reliance on digital data. A thorough framework for "Enhancing Data Protection through Advanced Encryption" (EDPAE) is introduced in this study. The project's goal is to protect sensitive data by utilizing state-of-the-art encryption techniques in response to the ever-changing cyber security scenario. In addition, the project places a strong emphasis on how to seamlessly incorporate advanced encryption into current data storage and communication systems in order to minimize interference with user operations and greatly improve overall security posture. In order to guarantee the secure creation, distribution, and storage of encryption keys and to reduce potential risks related to key compromise, key management features are addressed.

I. INTRODUCTION

The protection of sensitive data has become extremely important in an era where technology permeates every aspect of our life. Strong data protection measures are absolutely necessary, as evidenced by the growing sophistication and frequency of cyber-attacks. A reliable line of defense against all of these is encryption, which offers a safe shield against illegal access, data breaches, and the possible compromise of private data. By offering a thorough framework named "Enhancing Data Protection through Advanced Encryption" (EDPAE), this study sets out to address the current issues related to data protection. Malicious actors looking to take advantage of weaknesses in digital systems have access to increasingly sophisticated tools as technology develops. EDPAE aims to expand on the parameters of We cover a wide range of topics related to advanced encryption, including safe multi-party computation, Currently, various security techniques are being implemented in fog computing, each with its respective pros and cons. In Fog Computing, the Decoy framework is being utilized as the existing security framework for data authentication. The decoy framework is designed as a system of deception, wherein counterfeit components are strategically deployed to entice unauthorized users, thereby restricting unauthorized access to the network. It is a cycle where the records are filled with decoys and are included by the service provider. This decoy framework comprises counterfeit records with sensitive names, such as social security numbers and credit card details, used as file names. These decoy components are designed to be enticing to potential attackers, who may click on them and attempt to download the file. Once the file is downloaded, an alert is triggered, notifying the system of the attack. This decoy framework strategy has been integrated with client behavior profiling, ensuring that any unauthorized access is promptly reported to the system. There are still a few issues with the current strategy, leading to hacking and unauthorized access to information in the fog. This has prompted us to consider data encryption in the fog framework. Therefore, with this approach, our aim is to achieve enhanced security at the Fog tier by introducing encryption to the data using a Hybrid Encryption algorithm combined with a machine learning model. The paper introduces the proposed security model algorithm in the Fog environment. According to this model, when the user sends data to the Fog for storage in the cloud, the data will be encrypted by the Fog before transmission to the cloud. Additionally, whenever the client requests the data,the encrypted information travels from the cloud to the fog and finally to the end-user, where it will be decrypted quantum-resistant cryptography, and holomorphic encryption. All these elements work together to achieve the main objective of building a strong defense system that can not only repel dangers that are already there but also foresee and lessen those that are coming. EDPAE aims to make sophisticated encryption a useful and intuitive part of regular digital interactions by integrating seamlessly with current data storage and communication platforms. In this way, it aims to close the gap that exists between increased data protection and user convenience by making sure that security measures improve rather than hinder user operations. With a closer look at the EDPAE architecture, this study seeks to shed light on how advanced encryption might be used to strengthen.

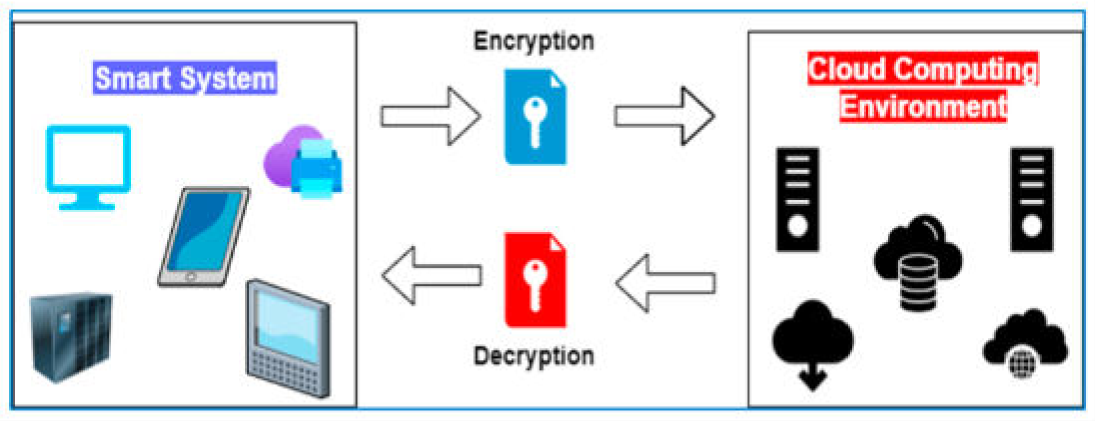
1. Key distribution in the original has serious weaknesses since keys are transmitted over the air or preinstalled onto devices in an insecure manner. Additionally, all nodes share the same key, which puts the entire network at risk if a single node is compromised. Our solution addresses these shortcomings by utilizing a one-time-use session key and a secure dynamic array of bits to secure communication between two nodes, ensuring they cannot be used for future communications.
2. We introduce a novel mutual authentication approach for wireless sensor networks.
3. This paper proposes a solution to strengthen the encryption between D2TC and D2D communication in wireless sensor networks.
4. The proposed approach achieves protection against various attacks by relying on simple operations rather than computationally expensive cryptographic operations.

II. RELATED WORK

Cyber security work in the realm of enhancing data protection through advanced encryption or improving data security with advanced encryption encompasses a variety of approaches, techniques, and research efforts aimed at bolstering the security of sensitive information. Here, we'll explore several key areas of related work in this field:

1. **Homomorphic Encryption**: Homomorphic encryption allows computations to be performed on encrypted data without decrypting it first. This technique has gained traction in recent years due to its potential to enable secure data processing in outsourced or cloud environments. Various research efforts have focused on optimizing and scaling homomorphic encryption schemes to make them practical for real-world applications.
2. **Post-Quantum Cryptography**: With the advent of quantum computers, traditional encryption algorithms such as RSA and ECC face the risk of being broken. Post-quantum cryptography aims to develop encryption schemes that are secure against attacks from quantum computers. Research in this area includes the exploration of lattice-based, code-based, and hash-based cryptographic primitives, among others.
3. **Secure Multi-Party Computation (MPC)**: MPC protocols allow multiple parties to jointly compute a function over their inputs while keeping those inputs private. Advanced encryption techniques play a crucial role in enabling secure computation in MPC settings. Recent research has focused on improving the efficiency and scalability of MPC protocols, making them applicable to a wider range of use cases.
4. **Fully Homomorphic Encryption (FHE)**: FHE schemes enable computations on encrypted data with no information leakage about the plaintext. While FHE was once considered prohibitively slow for practical use, recent advancements have made it more feasible. Researchers continue to explore optimizations and novel constructions to further improve the performance and usability of FHE.
5. **Attribute-Based Encryption (ABE)**: ABE allows access control policies to be embedded directly into ciphertexts, enabling fine-grained access control over encrypted data. Research in this area has focused on developing efficient ABE schemes for various access control scenarios, such as role-based access control and attribute-based access control.
6. **Hardware-based Encryption**: Hardware-based encryption solutions leverage dedicated cryptographic hardware to accelerate encryption and decryption operations while ensuring the security of sensitive data. Recent advancements in hardware security modules (HSMs), trusted execution environments (TEEs), and secure enclaves have enhanced the security and performance of hardware-based encryption solutions.

Figure 1. The smart system's general model of secure data offloading to the cloud computing environment.



IMPLEMENTATION AND FLOW DIAGRAM:

Step 1: Identify Data to be Encrypted.

- Identify sensitive data that requires encryption, such as personally identifiable information (PII), financial records, intellectual property, etc.
- Classify data based on its sensitivity level and regulatory requirements.

Step 2: Select Encryption Algorithms and Keys

- Choose suitable encryption algorithms based on security requirements and industry standards (e.g., AES, RSA, ECC).
- Generate strong encryption keys and establish key management practices to securely store and manage keys

Step 3: Implement Encryption Mechanism

- Integrate encryption mechanisms into data storage systems, databases, applications, and communication channels.
- Utilize encryption libraries or modules provided by programming languages or third-party vendors.

Step 4: Data Encryption Process

- When data is created or collected, encrypt it using the selected encryption algorithm and key.
- Ensure encryption is performed before data is stored or transmitted over networks.

Step 5: Key Management and Storage

- Implement robust key management practices to safeguard encryption keys.
- Store encryption keys securely, utilizing hardware security modules (HSMs), key management servers, or secure key vaults

Step 6: Access Control and Authentication

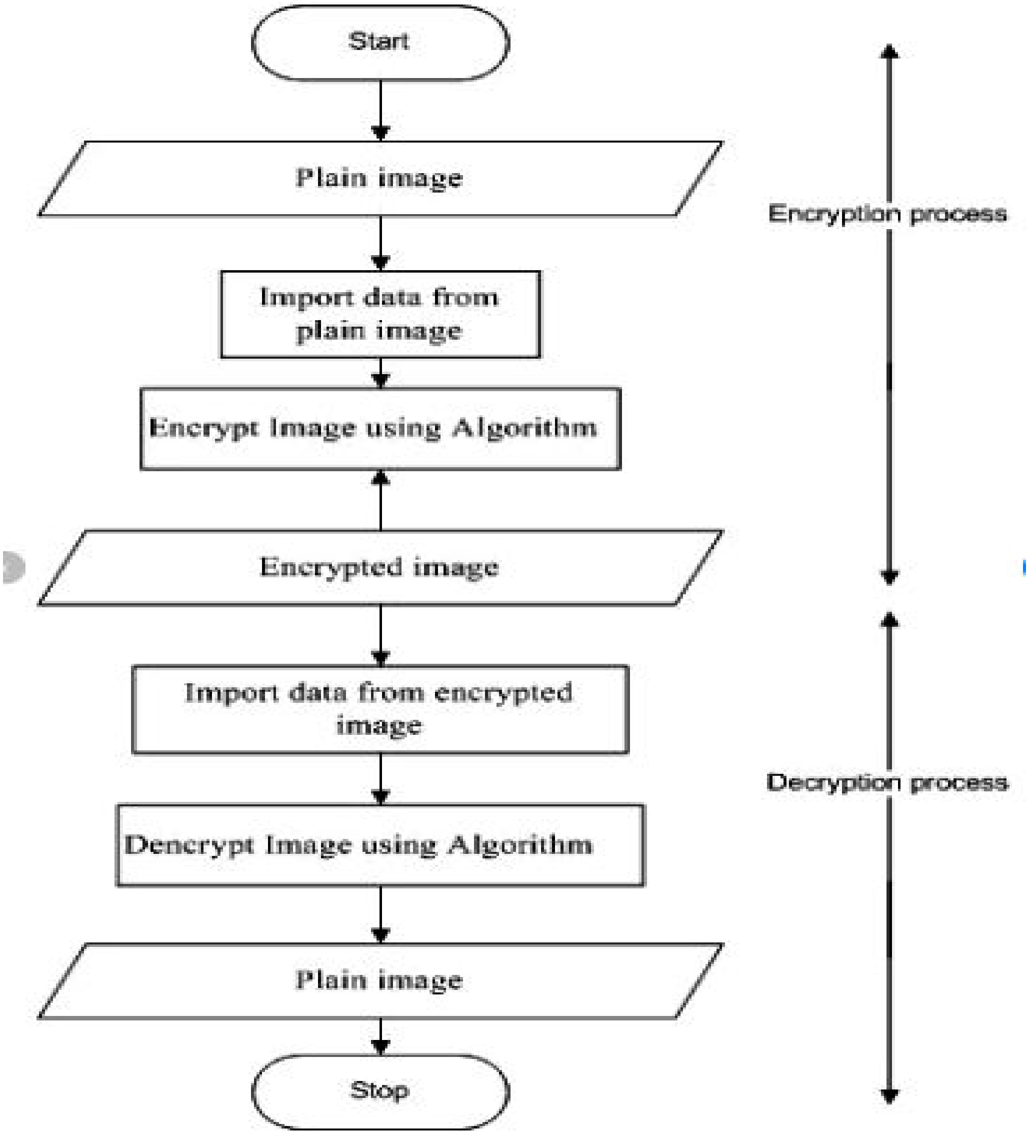
- Enforce strict access controls to limit access to encrypted data.
- Authenticate users and applications before granting access to decryption keys or encrypted data

Step 7: Monitoring and Auditing

- Implement monitoring mechanisms to detect unauthorized access attempts or unusual activities related to encryption.
- Conduct regular audits to ensure compliance with encryption policies and regulatory requirements.

Flow Diagram:

[Start] --> [Identify Data to be Encrypted] --> [Select Encryption Algorithms and Keys]
--> [Implement Encryption Mechanism] --> [Data Encryption Process] --> [Key Management and Storage]
--> [Access Control and Authentication] --> [Monitoring and Auditing] --> [End]

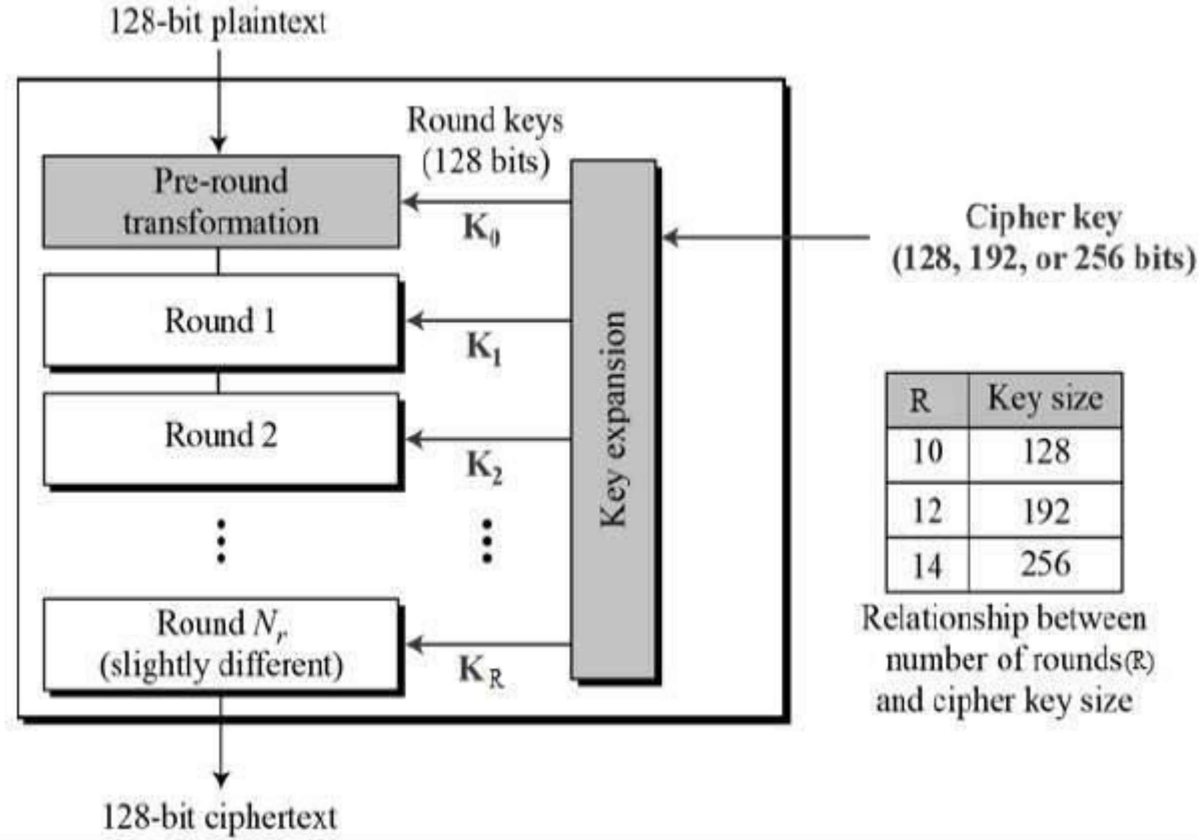

Start
Plain image
Import data from plain image
Encrypt Image using Algorithm
Encrypted image
Import data from encrypted image
Dencrypt Image using Algorithm
Plain image
Stop
Encryption process
Decryption process

III. METHODOLOGY

The methodology for enhancing data protection through advanced encryption or improving data security with advanced encryption typically involves several key steps. First, a thorough assessment of existing data security measures is conducted to identify vulnerabilities and areas for improvement. Next, suitable encryption algorithms and protocols are selected based on the sensitivity of the data and compliance requirements. Implementation involves integrating encryption techniques into relevant systems and applications, ensuring compatibility and minimal performance impact. Ongoing monitoring and updates are essential to address emerging threats and maintain effectiveness. Additionally, staff training and awareness programs may be implemented to ensure proper encryption usage and data handling practices.

1. **Understanding Data Assets**: Begin by comprehensively identifying and categorizing all data assets within the organization. This includes sensitive information such as customer data, financial records, intellectual property, and any other proprietary information.
2. **Risk Assessment**: Conduct a thorough risk assessment to identify potential vulnerabilities and threats to the data assets. This involves analyzing the likelihood and potential impact of various security breaches, including unauthorized access, data theft, and cyber-attacks.

3. **Encryption Requirements Analysis**: Determine the specific encryption requirements based on the sensitivity and regulatory requirements of the data. This involves identifying the types of encryption algorithms and key management practices necessary to adequately protect the data.
4. **Encryption Algorithm Selection**: Evaluate different encryption algorithms based on factors such as security strength, performance impact, and compatibility with existing systems. Choose algorithms that offer strong protection against both current and future threats.
5. **Key Management Strategy**: Develop a comprehensive key management strategy to securely generate, store, and distribute encryption keys. This includes defining key lifecycle management processes, access controls, and encryption key rotation policies.
6. **Data Encryption Implementation**: Implement encryption mechanisms at various layers of the data infrastructure, including databases, file systems, communication channels, and endpoint devices. Ensure that encryption is seamlessly integrated into existing workflows and applications.
7. **Data in Transit Encryption**: Implement secure communication protocols such as TLS/SSL to encrypt data transmitted between servers, clients, and other endpoints. This prevents eavesdropping and man-in-the-middle attacks during data transmission.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Literature Review

This literature review explores the efficacy of advanced encryption techniques in enhancing data protection and improving overall data security. By examining existing research, this review aims to provide insights into the role of encryption in safeguarding sensitive information against unauthorized access and cyber threats

Encryption as a Fundamental Tool for Data Protection: Encryption serves as a fundamental tool for protecting data both at rest and in transit (Barker et al., 2016). By encoding information in a cryptographic format, encryption ensures that even if data is intercepted, it remains unintelligible to unauthorized parties. Advanced encryption algorithms, such as AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman), provide robust mechanisms for securing data against various forms of cyber threats, including eavesdropping and data breaches (Biryukov et al., 2016). The Role of Encryption in Regulatory Compliance: Encryption plays a crucial role in ensuring compliance with data protection regulations and standards, such as GDPR (General Data Protection Regulation) and HIPAA (Health Insurance Portability and Accountability Act) (Dhillon et al., 2019). By encrypting sensitive data, organizations can mitigate the risk of non-compliance penalties and safeguard the privacy rights of individuals. Moreover, encryption facilitates secure data sharing and collaboration while maintaining regulatory compliance requirements. Challenges and Limitations of Advanced Encryption: Despite its effectiveness, advanced encryption faces certain challenges and limitations in practice. Key management and distribution present significant hurdles, as organizations struggle to securely manage encryption keys and ensure their timely rotation (Samarati & De Capitani di Vimercati, 2001). Moreover, the computational overhead associated with encryption and decryption processes can impact system performance, especially in resource-constrained environments. Advancements in Quantum Encryption: The emergence of quantum computing poses a potential threat to traditional encryption schemes, as quantum computers have the capability to break conventional cryptographic algorithms (Mosca, 2018). In response, researchers are exploring quantum-resistant encryption techniques, such as lattice-based cryptography and hash-based signatures, to mitigate the vulnerabilities posed by quantum computing (Albrecht et al., 2019). However, the practical implementation and scalability of quantum-resistant encryption remain areas of ongoing research and development

IV. CONCLUSION

A proactive and flexible solution to the constantly changing landscape of cyber security threats is the "Enhancing Data Protection through Advanced Encryption" (EDPAE) framework. The significance of consistently improving data protection methods in the face of persistent and sophisticated attacks is highlighted by our investigation of advanced encryption standards, state-of-the-art cryptographic algorithms, and robust key management systems. The path taken by this research has demonstrated the promise of sophisticated encryption techniques, such as safe multi-party computation, homomorphic encryption, and quantum-resistant cryptography. In addition to fixing existing flaws, these developments set up data security plans to survive upcoming difficulties like the emergence of quantum computing. The EDPAE framework aims to reconcile enhanced security with user comfort by incorporating advanced encryption into data storage and transmission systems in a smooth and seamless manner.

REFERENCES

1. G. Singh and Supriya, "A study of encryption algorithms (RSA DES 3DES and AES) for information security", International Journal of Computer Applications, vol. 67, pp. 33-38, April 2013.
2. P. S. Mukesh, M. S. Pandya and S. Pathak, "Enhancing AES algorithm with arithmetic coding", 2013 International Conference on Green Computing Communication and Conservation of Energy (ICGCE), pp. 83-86, 2013.
3. B. Padmavathi and S. R. Kumari, "A Survey on Performance Analysis of DES AES and RSA Algorithm along with LSB Substitution", International Journal of Science and Research (IJSR), vol. 2, pp. 170-174, April 2013
4. Z. Musliyana, T. Y. Arif and R. Munadi, "Security Enhancement of Advanced Encryption Standard (AES) using Time-Based Dynamic Key Generation", ARPN Journal of Engineering and Applied Sciences, vol. 10, pp. 8347-8350, October 2015.
5. Janadi and D. A. Tarah, "AES immunity Enhancement against algebraic attacks by using dynamic S-Boxes", 3rd International Conference on Information and Communication Technologies: From Theory to Applications.
6. V. Kaul, B. Nemade and V. Bharadi, "Next Generation Encryption Using Security Enhancement Algorithms for End to End Data Transmission in 3G/4G Networks", Procedia Computer Science, vol. 79, pp. 1051-1059, 2016.
7. H. Alanazi, B. B. Zaidan, A.A. Zaidan, H.A. Jalab, M. Shabbir and Y. Ai-Nabhani, "New comparative study between DES 3DES and AES within nine factors", Journal of Computing, vol. 2, pp. 152-157, March 2010.
8. Rivest, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.
9. Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644-654.
10. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons.
11. Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. John Wiley & Sons.
12. Katz, J., & Lindell, Y. (2014). Introduction to Modern Cryptography: Principles and Protocols. CRC Press.
13. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson Education.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details