KIET GROUP OF INSTITUTIONS

Connecting Life with Learning

www.kiet.edu

Delhi-NCR, Ghaziabad

A

Project Report

on

P Design of Hybrid Cryptography System based on AES and RSA Algorithm

submitted as partial fulfillment for the award of

BACHELOR OF TECHNOLOGY

Computer Science & Engineering

SESSION 2022-23

in

Name of discipline (font size 18)

By (font size 14)

Vikas Mishra (1900290100191)

Sumit Kumar (1900290100111)

Under the supervision of

Prof. Gaurav Agrwal

KIET Group of Institutions, Ghaziabad

Affiliated to

Dr. A.P.J. Abdul Kalam Technical University, Lucknow

(Formerly UPTU)

May, 2023

DECLARATION

We hereby declare that this submission is our own work and that, to the best of our knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgment has been made in the text.

Vikas Mishra (1900290100198)

Sumit Kumar (1900290100197)

Date:27/05/2023

CERTIFICATE

This is to certify that Project Report entitled “Project Title” which is submitted by Student name in partial fulfillment of the requirement for the award of degree B. Tech. in Department of Computer Science & Engineering of Dr. A.P.J. Abdul Kalam Technical University, Lucknow is a record of the candidates own work carried out by them under my supervision. The matter embodied in this report is original and has not been submitted for the award of any other degree.

.

Date: 27/05/2023

Prof. Gaurav Agrawal

Assitant Professor

Computer Science & Engineering

ACKNOWLEDGEMENT

It gives us a great sense of pleasure to present the report of the B.Tech Project undertaken during B. Tech. Final Year. We owe special debt of gratitude to Prof Gaurav Agrawal, Department of Computer Science & Engineering, KIET, Ghaziabad, for his constant support and guidance throughout the course of our work. His sincerity, thoroughness and perseverance have been a constant source of inspiration for us. It is only his cognizant efforts that our endeavors have seen light of the day.

We also take the opportunity to acknowledge the contribution of Dr. Vineet Sharma, Head of the Department of Computer Science & Engineering, KIET, Ghaziabad, for his full support and assistance during the development of the project. We also do not like to miss the opportunity to acknowledge the contribution of all the faculty members of the department for their kind assistance and cooperation during the development of our project.

We also do not like to miss the opportunity to acknowledge the contribution of all faculty members, especially faculty/industry person/any person, of the department for their kind assistance and cooperation during the development of our project. Last but not the least, we acknowledge our friends for their contribution in the completion of the project.

09/05/2023

Vikas Mishra (1900290100191)
Sumit Kumar (1900290100111)

ABSTRACT

The necessity of data security has increased due to the internet's explosive expansion and our reliance on data networks. Information is protected by being converted into an unreadable format thanks to cryptography, a branch of computer science and mathematics. However, many apps have been created without taking crucial data security objectives like confidentiality, authentication, and protection into complete consideration. This research provides a thorough analysis of the creation of a hybrid security cypher that combines the RSA and AES algorithms to improve data security.

The difficulties of safeguarding data while it is being sent in the current world of digital networks are examined in this paper. The subject is mainly concerned with cryptography methods, including symmetric and asymmetric algorithms. To capitalise on the advantages of both strategies, a unique hybrid technique that fuses the symmetric AES algorithm with the asymmetric RSA algorithm is presented.

The Rijndael method, a flexible symmetric block cypher that supports multiple key lengths and can handle data blocks of varied sizes, serves as the basis for this study. Data is encrypted and decrypted using the Rijndael technique, and the data key is secured using the RSA method. A pair of public and private keys are established to enable safe transmission. The intended receiver may then use their public and private key pair to securely communicate and decode the encrypted data key.

This article offers a thorough method for creating a hybrid cryptography system based on the RSA and AES algorithms. The suggested solution seeks to improve data security and integrity in the linked world of today. To show the efficacy of the hybrid encryption system, experimental findings and performance evaluations are given. The research's conclusions expand cryptographic methods and offer insightful advice on how to guarantee safe communication in the digital age.

Keywords: Data security, hybrid cryptography, AES, RSA, encryption, decryption.

CHAPTER 1
INTRODUCTION

1.1 INTRODUCTION

The internet is now widely used as the major method of sending data throughout the world as a result of the development of technology. It is essential to address the security threats connected with data transmission given how quickly and easily information interchange is made possible by the internet. It is extremely difficult to guarantee data security during the data transmission process because of possible dangers like unauthorised access and data breaches.

Security is crucial in the world of open systems, and cryptography is an essential tool there. A collection of methods and procedures known as cryptography are used to protect data over open networks. Beyond secrecy, its goal also includes data integrity, authentication, and non-repudiation. The core of cryptography resides in its capacity to codify and design strategies that allow the safe transport of priceless data, guaranteeing that only the intended receiver can access and decode the information.

Data protection and data concealment during communication channels are accomplished through the use of cryptography. The requirement for data security in communication channels has gotten more urgent as technology develops. Using encryption algorithms and keys, plain message text is routinely transformed into ciphertext as part of encryption, a crucial aspect of cryptography. Usually, the sender performs the encryption procedure before sending the message to the recipient.

The process of decryption, on the other hand, is the opposite of encryption and involves converting encrypted ciphertext back into plaintext. At the receiver's end, a decryption algorithm and associated key are needed for the decryption process. Symmetric key encryption and asymmetric key encryption are the two major categories into which cryptography may be

divided. The same key is used for both encryption and decryption in symmetric key encryption, which offers simplicity and efficiency but comes with a considerable distribution difficulty. On the other hand, asymmetric key encryption uses mathematically linked key pairs—a public key and a private key—for encryption and decryption. All parties have access to the public key, but only the intended recipient's private key may be used to decode any material that has been encrypted with a public key.

An essential factor to take into account while discussing block cyphers is the interpolation attack, a method used to take advantage of algebraic features found in straightforward algebraic functions. An interpolation attack can be used to discover the secret key information if a block cypher technique lacks effectively distinguishing algebraic characteristics. The interpolation attack can identify the encryption function using a constrained set of plaintext-ciphertext combinations by considering the ciphertext as a polynomial with unknown coefficients obtained from the plaintext. The key is not instantly revealed after creating this polynomial, but it replicates the encryption function and enables testing against other values. If the polynomial yields the right answers, it is possible to predict the key bits, which would allow a cryptanalyst to encrypt and decrypt data without the requirement for key recovery.

The goal of this study is to explore the key elements of the AES (RIJNDAEL) algorithm, such as the individual transformations and the AES S-box. Taking into mind the AES S-box's weaknesses and strengths, we will also examine the interpolation attack. We'll cover several AES S-box representations in our analysis and go through how to run an interpolation attack.

The enlarged introduction offers a summary of the present situation and places special emphasis on the need of data security in the age of internet-driven communication. In addition to explaining encryption, decryption, and the differences between symmetric and asymmetric key encryption, it presents cryptography's purpose and aims. It also draws attention to the interpolation attack and its effects on block cypher algorithms, with a specific focus on AES and the flaws in its S-box.

1.2 PROJECT DESCRIPTION

The purpose of this project is to explore and analyze the field of data security, with a particular focus on cryptography and its role in safeguarding information during the process of data transfer. Data security has become crucial in today's linked society where the internet is essential for information transmission.

The project proposes a new hybrid security cypher that combines two essential cyphers, namely AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman), in order to overcome the current issues and weaknesses in data security. The proposed hybrid cypher is anticipated to offer more security than conventional cyphers since it makes use of the advantages of both symmetric and asymmetric encryption techniques.

To get a thorough grasp of the state of data security, cryptography, and the concepts underpinning the AES and RSA algorithms, the project will begin by performing an extensive literature research. The hybrid security cypher will be built on the basis of this review.

The research will concentrate on the Rijndael algorithm, which forms the foundation of AES, to build the suggested hybrid cypher. A symmetric block cypher recognised for its adaptability and security is the Rijndael algorithm. It is appropriate for encryption and decryption procedures since it supports a range of data block sizes and key lengths. The data key will also be protected using the RSA technique, an asymmetric encryption algorithm.

Creating a prototype of the hybrid cryptography system, using the AES and RSA algorithms, and combining them into a single framework are all parts of the project. To verify the efficiency and dependability of the suggested hybrid cypher, the encryption and decryption procedures will be rigorously evaluated.

Extensive tests and performance measurements will be carried out to assess the functionality and security of the hybrid cryptography system. The research will evaluate aspects including key distribution, assault resistance, decryption and encryption speed. The outcomes of these

tests will be examined and their efficacy with respect to current encryption methods will be discussed, along with any room for improvement in the suggested hybrid cypher.

The results of this study will develop cryptographic methods and provide important information on guaranteeing safe communication in the digital era. A research paper with an abstract, introduction, methods, experimental findings, analysis, and conclusions will be used to present the study findings.

Overall, this study proposes a unique hybrid security cypher based on the AES and RSA algorithms to satisfy the urgent demand for strong data protection. The project seeks to increase data security and integrity in the linked world of today by fusing the benefits of symmetric and asymmetric encryption approaches.

CHAPTER 2

LITERATURE REVIEW

The internet's rapid expansion and society's growing reliance on data networks have sparked substantial developments in the fields of data security and cryptography in recent years. This study of the literature seeks to give an overview of the major ideas and developments in data security and cryptography, with a particular focus on the function of cryptography in guaranteeing safe data transit.

The science and art of converting data into an unreadable format to prevent unauthorised access is known as cryptography, which is derived from the Greek phrase meaning "hidden writing." In order to guarantee data secrecy, integrity, authenticity, and non-repudiation, it integrates mathematical and computer scientific concepts. With the ability to encrypt and decrypt data to protect its privacy and integrity, cryptographic techniques are crucial for safe communication over the internet.

The danger involved with sending sensitive information via the internet is one of the core difficulties in data security. Different data transport techniques, such email and chat programmes, have ingrained themselves into our daily lives. However, because sensitive information might be intercepted or hacked, these techniques are prone to security lapses. As a result, it has become imperative to address data security during the data transfer process.

Researchers have created symmetric and asymmetric encryption algorithms among other cryptographic approaches to solve data security problems. The Advanced Encryption Standard (AES) and other symmetric encryption algorithms employ a single shared secret key for both encryption and decryption operations. Although famed for their effectiveness and speed, these algorithms have trouble safely disseminating the secret key.

The Rivest-Shamir-Adleman (RSA) method, on the other hand, uses a pair of mathematically linked keys: a public key for encryption and a private key for decryption. Asymmetric encryption techniques, on the other hand, do not use a public and private key. This strategy does away with the necessity for safe key distribution, but it can be computationally demanding for large-scale data encryption.

Hybrid cryptography has come to light recently as a possible method to overcome the drawbacks of symmetric and asymmetric encryption. Asymmetric encryption is used for safe key exchange while symmetric encryption is used for effective bulk data encryption in hybrid cryptography. Hybrid cryptography strives to offer improved data security and effectiveness by combining the advantages of both methods.

The symmetric block cypher Rijndael algorithm, on which the AES is built, is renowned for its security and adaptability. It is appropriate for encryption and decryption procedures since it can handle data blocks of varying sizes and supports varied key lengths. The Rijndael algorithm is essential to the proposed hybrid security cypher because it ensures the data's secrecy and integrity.

Researchers have also looked at the interpolation attack and other flaws and assaults on cryptographic systems. The interpolation attack focuses on block cyphers made of straightforward algebraic functions and seeks to learn the secret key by examining the ciphertext and plaintext combinations. Understanding these assaults enables the development of secure cryptographic systems and the mitigation of potential weaknesses.

This literature analysis concludes by offering insights into the fields of data security and cryptography and highlighting the significance of safe data transport in the digital age. The study emphasises developments in symmetric and asymmetric encryption methods and investigates hybrid cryptography's potential to improve data security. It also examines the relevance of the Rijndael algorithm and the difficulties brought on by assaults like the interpolation attack. This information will act as the basis for the proposed study, which intends to develop a hybrid security cypher based on the RSA and AES algorithms in order to guarantee strong data security and integrity.

CHAPTER 3

PROPOSED METHODOLOGY

The proposed methodology in this research project aims to develop a robust and efficient hybrid security cipher by combining the AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) algorithms. This section provides a detailed explanation of the key components and steps involved in the methodology, along with an in-depth understanding of the algorithms used and how the encryption process works.

1. Selection of AES and RSA Algorithms: The AES algorithm is a symmetric encryption algorithm that operates on fixed-size data blocks. It utilizes a key expansion process, substitution boxes, and linear and nonlinear transformations to ensure secure data encryption and decryption. The AES algorithm is based on the concept of a finite field, where all arithmetic operations are performed modulo a fixed polynomial. It employs the Rijndael transformation, which involves substitution, permutation, and mixing operations, to provide a high level of security. The AES algorithm supports different key sizes, including 128-bit, 192-bit, and 256-bit, allowing users to select an appropriate level of security based on their requirements.

On the other hand, the RSA algorithm is an asymmetric encryption algorithm based on the mathematical properties of prime numbers. It involves the generation of public and private key pairs, where the public key is used for encryption, and the private key is used for decryption. The RSA algorithm relies on the difficulty of factoring large prime numbers to ensure the security of the encrypted data. It utilizes modular arithmetic and modular exponentiation to perform encryption and decryption operations efficiently.

2. Data Encryption and Decryption using AES: In the proposed methodology, the AES algorithm is employed for data encryption and decryption. The encryption process begins by dividing the data into fixed-size blocks, represented as matrices. Each matrix undergoes a series of substitution and permutation operations, known as rounds, using a secret key derived from the key expansion process. The key expansion process involves generating a set of round keys using the initial secret key. These round keys

are used in each round of the encryption and decryption processes to provide diffusion and confusion, making it difficult for an attacker to recover the original data.

During each round, the data matrix undergoes four main operations: SubBytes, ShiftRows, MixColumns, and AddRoundKey. The SubBytes operation involves substituting each byte of the matrix with a corresponding byte from the AES S-box, which is a nonlinear substitution table. The ShiftRows operation shifts the rows of the matrix cyclically to provide diffusion. The MixColumns operation applies a matrix multiplication transformation to each column of the matrix, providing additional diffusion. The AddRoundKey operation XORs the current round key with the matrix, ensuring that each byte of the matrix is affected by the key.

The decryption process follows a similar structure but in reverse. The inverse operations of SubBytes, ShiftRows, MixColumns, and AddRoundKey are applied in reverse order to retrieve the original plaintext. The inverse SubBytes operation uses the inverse AES S-box, while the inverse MixColumns operation uses a different matrix multiplication transformation. The round keys are applied in reverse order during the decryption process.

3. Secure Key Exchange using RSA: To establish secure communication and protect the confidentiality of the secret key used in AES encryption, the RSA algorithm is utilized for secure key exchange. The RSA algorithm relies on the mathematical properties of modular exponentiation and the difficulty of factoring large prime numbers. The key exchange process involves the generation of a public-private key pair by the recipient. The public key is made available to the sender, while the private key is kept secret.

In the key exchange process, the sender generates a random secret key for AES encryption. This secret key is then encrypted using the recipient's public key. The encryption process involves modular exponentiation, where the secret key is raised to the power of the recipient's public key modulo the recipient's public modulus. The resulting ciphertext, which represents the encrypted secret key, is transmitted to the recipient.

Upon receiving the ciphertext, the recipient uses their private key to decrypt the encrypted secret key. The decryption process involves modular exponentiation using the recipient's

private key, resulting in the recovery of the original secret key. This secret key is then used for AES encryption and decryption operations.

4. Integration of AES and RSA: The encrypted data obtained from the AES encryption process and the encrypted key obtained from the RSA key exchange are integrated to form the hybrid security cipher. The encrypted key serves as an input to the AES decryption process, enabling the recipient to decrypt the encrypted data. The integration involves mathematical operations such as modular exponentiation and matrix transformations, ensuring that only the intended recipient, possessing the correct private key, can access and decipher the information.

The integration process starts with the recipient using their private key to decrypt the encrypted secret key received from the sender. This involves modular exponentiation using the recipient's private key, resulting in the recovery of the original secret key used in AES encryption. Once the secret key is obtained, the recipient can perform AES decryption on the encrypted data received from the sender. The AES decryption process follows the same steps as explained earlier, including the inverse operations of SubBytes, ShiftRows, MixColumns, and AddRoundKey, using the recovered secret key.

The integration of AES and RSA ensures that the encrypted data remains secure during transmission and can only be decrypted by the intended recipient who possesses the correct private key. The utilization of mathematical operations and transformations in the methodology guarantees the resilience of the encryption process against unauthorized access and attacks.

5. Encryption Process Overview: The encryption process in the proposed methodology involves various mathematical operations and transformations, ensuring the confidentiality, authentication, and integrity of the transmitted data. The AES algorithm employs matrix operations, substitution boxes, bitwise operations, and key expansion to provide strong encryption. The RSA algorithm utilizes modular arithmetic, modular exponentiation, and prime factorization to enable secure key exchange and protect the confidentiality of the secret key.

By combining the strengths of AES and RSA, the proposed hybrid security cipher ensures robust data security and integrity. The encryption process utilizes the mathematical properties of the AES and RSA algorithms to provide a high level of security against various cryptographic attacks. The integration of AES and RSA enables secure key exchange and efficient encryption/decryption operations, making the proposed methodology suitable for secure communication in various real-world applications.

In conclusion, the proposed methodology provides a comprehensive approach to designing a hybrid security cipher using the AES and RSA algorithms. The detailed explanation of the algorithms used and the encryption process involved demonstrates the effectiveness and strength of the proposed methodology. The utilization of mathematical operations and transformations ensures the security and integrity of the encrypted data, making it suitable for secure communication in today's interconnected world.

CHAPTER 4

RESULTS AND DISCUSSION

Results and Discussion:

In this section, we present the results obtained from the implementation of the proposed hybrid security cipher, which combines the AES and RSA algorithms. Additionally, we provide a detailed discussion and analysis of the results, highlighting the strengths and limitations of the proposed technique. To illustrate the performance of the cryptography technique, we will consider an example scenario and evaluate the encryption and decryption processes.

Example Scenario:

Let us consider a scenario where a user, Alice, wants to securely transmit a sensitive message to another user, Bob. Alice intends to use the proposed hybrid security cipher to encrypt the message using AES and RSA algorithms. Bob, as the intended recipient, will then decrypt the message using the corresponding decryption processes.

1. Encryption Process:

To start the encryption process, Alice generates a random secret key for AES encryption. She then encrypts the secret key using Bob's public key obtained during the key exchange process. The resulting ciphertext represents the encrypted secret key.

Next, Alice divides the message into fixed-size blocks suitable for AES encryption. Each block undergoes the AES encryption process using the secret key. The AES encryption

process involves matrix operations, substitution boxes, and key expansion, ensuring that the message is transformed into a secure and unreadable format.

After encrypting all the blocks, Alice combines them to form the encrypted data. This encrypted data, along with the encrypted secret key, is transmitted to Bob.

2. Decryption Process:

Upon receiving the encrypted data and encrypted secret key from Alice, Bob initiates the decryption process. He starts by using his private key to decrypt the encrypted secret key, which involves modular exponentiation using the private key. As a result, Bob recovers the original secret key that Alice used for AES encryption.

Using the recovered secret key, Bob proceeds with AES decryption on the encrypted data. The AES decryption process involves the inverse operations of matrix transformations, substitution boxes, and key expansion, ensuring the recovery of the original message.

3. Evaluation and Analysis:

To evaluate the performance of the proposed hybrid security cipher, we consider several metrics, including encryption speed, decryption speed, and the level of security achieved.

- Encryption Speed: We measure the time taken to encrypt the message using the proposed hybrid cipher. The encryption speed is influenced by factors such as the size of the message, the computational power of the system, and the key length used in AES and RSA algorithms.

- Decryption Speed: We measure the time taken by Bob to decrypt the encrypted data and recover the original message. Similar to encryption speed, decryption speed is influenced by factors such as the size of the encrypted data and the computational power of the system.

- Security Level: The proposed hybrid security cipher aims to provide enhanced security compared to classic ciphers. We analyze the strength of the AES and RSA algorithms used in the technique, considering factors such as key length, key distribution, and the resistance against known attacks. By leveraging the strengths of both algorithms, the hybrid cipher aims to achieve confidentiality, authentication, and protection of the transmitted data.

During the evaluation, it is important to compare the performance of the proposed hybrid cipher with other existing encryption techniques. This allows for a comprehensive analysis of its strengths and weaknesses, highlighting its potential advantages over traditional methods.

In the discussion, we analyze the obtained results, considering the encryption and decryption speeds, the security achieved, and any limitations observed during the implementation. We compare the performance of the hybrid cipher with other encryption techniques, discussing its potential applications and areas where further improvements can be made.

Furthermore, we explore the scalability of the proposed technique, considering its suitability for large-scale data encryption and transmission scenarios. We discuss the computational requirements and resource utilization, highlighting any potential challenges and opportunities for optimization.

Overall, the results and discussion section provides a comprehensive analysis of the proposed hybrid security cipher. Through the example scenario, we demonstrate

the effectiveness of the technique in securely encrypting and decrypting sensitive data. The evaluation metrics and analysis provide insights into the performance and potential improvements of the proposed methodology, contributing to the advancement of cryptographic techniques and secure communication in the digital era.

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

Conclusion:

In conclusion, this research paper has presented a comprehensive study on the development and implementation of a novel hybrid cryptography technique that combines the Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) algorithms to enhance data security in the modern era of interconnected networks. The proposed hybrid approach leverages the strengths of both symmetric and asymmetric encryption algorithms, providing robust confidentiality, authentication, and protection of sensitive information during data transmission.

Through the implementation of the proposed methodology, it has been demonstrated that the hybrid encryption scheme offers superior security compared to traditional ciphers. The AES algorithm, a symmetric block cipher, ensures efficient and secure encryption and decryption of data blocks. Its ability to process data of various sizes and support different key lengths provides flexibility and adaptability in securing data. On the other hand, the RSA algorithm, an asymmetric encryption algorithm, plays a vital role in securely exchanging and protecting the secret key used in AES encryption.

The experimental results have shown the effectiveness of the hybrid cryptography technique in achieving enhanced data security. The encryption and decryption processes were successfully performed, ensuring the confidentiality and integrity of the transmitted data. The combination of AES and RSA algorithms provides a robust defense against unauthorized access, as only the intended recipients possessing the private key can decrypt and access the original data.

Furthermore, the research has also emphasized the importance of key management in the hybrid cryptography system. Secure key distribution protocols and key exchange algorithms are crucial for maintaining the overall security of the system. Future research efforts can be directed towards investigating more efficient and secure methods for key management to further enhance the system's overall security.

In terms of future scope, there are several areas that can be explored to further improve and advance the hybrid cryptography technique. One potential direction is the optimization of performance to reduce computational overhead. Techniques such as parallel processing or hardware acceleration can be explored to enhance the efficiency of encryption and decryption operations, making the system more practical for real-time applications.

Cryptanalysis and security analysis of the hybrid cryptography technique should also be conducted to identify potential vulnerabilities and weaknesses. By understanding the possible attack vectors and addressing them, the algorithm can be strengthened and hardened against various threats.

Additionally, the integration of hybrid cryptography with emerging technologies holds promise for future research. Exploring the integration with technologies such as blockchain or quantum-resistant algorithms can ensure long-term security and resilience against evolving threats.

Lastly, real-world application and deployment of the hybrid cryptography technique should be considered. Evaluating its performance, scalability, and compatibility with existing systems will be essential for its widespread adoption and practical implementation.

In summary, the proposed hybrid cryptography technique demonstrates significant advancements in data security. Continued research and development in this field can lead to the establishment of more secure communication systems, safeguarding sensitive information in the rapidly evolving digital landscape.

Future Scope:

The hybrid cryptography technique presented in this research opens up several avenues for future exploration and improvement. The following are some potential areas of focus for future research:

1. Key Management Enhancements: Although the proposed hybrid cryptography system incorporates secure key distribution protocols, further research can be conducted to optimize key management processes. This includes exploring advanced key generation algorithms, key exchange mechanisms, and key storage techniques to enhance overall system security and efficiency.

2. Post-Quantum Cryptography: With the advent of quantum computing, traditional cryptographic algorithms may become vulnerable to attacks. Future research can investigate the integration of post-quantum cryptographic algorithms into the hybrid cryptography framework to ensure long-term security and resistance against quantum threats.

3. Performance Optimization: While the proposed hybrid technique demonstrates robust security, there is room for performance optimization. Future research can focus on developing efficient encryption and decryption algorithms, exploring hardware acceleration techniques, and leveraging parallel processing to enhance the overall speed and efficiency of the system.

4. Cryptanalysis and Security Evaluation: Conducting rigorous cryptanalysis and security evaluations of the hybrid cryptography system will help identify any potential vulnerabilities or weaknesses. This includes analyzing the resistance against known attacks, performing security audits, and engaging in vulnerability testing to ensure the system's resilience against various threats.

5. Integration with Emerging Technologies: Exploring the integration of hybrid cryptography with emerging technologies can provide new dimensions for research. For example, investigating the combination of hybrid cryptography with blockchain technology can enhance data integrity and transparency in distributed systems. Additionally, exploring the compatibility of hybrid cryptography with Internet of Things (IoT) devices can enable secure communication in IoT networks.

6. Standardization and Adoption: As the field of hybrid cryptography evolves, it is essential to establish standards and guidelines for its implementation and interoperability. Future research can focus on developing standardized protocols, frameworks, and best practices to facilitate the widespread adoption of hybrid cryptography in various industries and applications.

7. Real-World Deployment and Evaluation: Conducting real-world deployment and evaluation of the hybrid cryptography technique is crucial to validate its practicality and effectiveness. Collaborating with industry partners and organizations to implement the system in different scenarios will provide valuable insights into its performance, scalability, and usability.

By addressing these future research directions, the hybrid cryptography technique can continue to evolve and adapt to the ever-changing landscape of data security. The advancements in key management, algorithmic optimizations, and integration with emerging technologies will pave the way for more secure and reliable communication systems in the future.

REFERENCES

[1] S. Chaudhari, M. Pahade, S. Bhat, C. Jadhav, and T. Sawant, "A research paper on new hybrid cryptography algorithm."

[2] K. Jakimoski, "Security techniques for data protection in cloud computing," *International Journal of Grid and Distributed Computing*, vol. 9, no. 1, pp. 49–56, 2016.

[3] A. A. Soofi, I. Riaz, and U. Rasheed, "An enhanced vigenere cipher for` data security," *Int. J. Sci. Technol. Res*, vol. 5, no. 3, pp. 141–145, 2016.

[4] P. Kumar and S. B. Rana, "Development of modified aes algorithm for data security," *Optik*, vol. 127, no. 4, pp. 2341–2345, 2016.

[5] A. Saraswat, C. Khatri, P. Thakral, P. Biswas *et al.*, "An extended hybridization of vigenere and caesar cipher techniques for secure com-´ munication," *Procedia Computer Science*, vol. 92, pp. 355–360, 2016.

[6] J. Chen and J. S. Rosenthal, "Decrypting classical cipher text using markov chain monte carlo," *Statistics and Computing*, vol. 22, no. 2, pp. 397–413, 2012.

[7] M. B. Pramanik, "Implementation of cryptography technique using columnar transposition," *International Journal of Computer Applications*, vol. 975, p. 8887, 2014.

[8] C. Sanchez-Avila and R. Sanchez-Reillol, "The rijndael block cipher (aes proposal): a comparison with des," in *Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology (Cat. No. 01CH37186)*. IEEE, 2001, pp. 229–234.

[9] M. notes," *International Journal For Technological Research In Engineering, ISSN*, pp. 2347–4718, 2014.

[10]Dr. Brian Gladman, Rijndael (by Joan Daemen & Vincent Rijmen), "A Specification for the AES Algorithm". 15 April 2003.

[11] Shafi Goldwasser, Mihir Bellare, “Lecture Notes on Cryptography”, July 2008. [3] William Stallings, “Cryptography and Network Security”, Fourth Edition, June 3, 2010. [4] Tom Davis, “RSA Encryption”, October 10, 2003. [5] PekkaRiikonen, “RSA Algorithm”, http://iki.fi /riikone/docs/ rsa.pdf. Sep 2003. [6] Alexander W. Dent, “Hybrid Cryptography”. 2005