iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** V **Month of publication:** May 2024

DOI: https://doi.org/10.22214/ijraset.2024.62420

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue V May 2024- Available at www.ijraset.com

Multi-Level Encryption System using AES and RSA Algorithms

Sheetal Phatangare[1], Shrinivas Jadhav[2], Sandesh Kawane[3], Prajwal Holkar[4], Pratiksha Gaikwad[5]
Department of Computer Engineering Vishwakarma Institute of Technology, Pune, Maharashtra, India

Abstract: ***As the volume of sensitive data entrusted to the cloud explodes, from healthcare records to financial transactions, the need for robust security solutions intensifies. Traditional encryption techniques, while effective, remain vulnerable to key compromise, leaving data exposed to malicious factors. This study proposes a multi-level encryption strategy that leverages the power of AES for efficient data encryption, RSA for secure key protection with public-key cryptography, and role-based encryption for granular access control. This layered approach significantly increases the computational complexity for unauthorized access, making brute-force or dictionary attacks exponentially more difficult. Our research demonstrates successful integration of these algorithms, achieving a 50% reduction in key compromise risk and enhanced data integrity through MAC verification. Moving forward, we envision seamless integration with multiple cloud platforms and exploring advanced access control mechanisms based on user context and behavior. This multi-level encryption strategy holds immense potential to reshape the landscape of cloud data security, fostering a more secure and trustworthy digital future.***
Keywords-AES, RSA, Roll-based encryption, Decryption, Cloud, security

I. INTRODUCTION

In our increasingly digital world, the safekeeping of sensitive data has become paramount. As more and more aspects of our lives migrate online, from financial transactions to personal communication and data storage, the need to protect this information from unauthorized access has become exponentially more critical. While cloud storage offers a convenient and scalable solution for data management, it introduces a new layer of complexity to the security landscape. A security breach in the cloud can have devastating consequences, leading to financial losses, reputational damage, and even legal repercussions.

Traditionally, data security has relied on encryption techniques like the Advanced Encryption Standard (AES). This widely used and highly secure symmetric-key encryption method transforms plain text data into unintelligible ciphertext, effectively shielding it from unwanted access. However, these techniques have a critical Achilles' heel: their dependence on a single encryption key. If this key falls into the wrong hands, the encrypted data becomes vulnerable to decryption, exposing sensitive information to potential harm.

Recognizing the limitations of single-layered encryption and the evolving security threats within the cloud environment, we propose a novel multi-level encryption strategy. This layered approach weaves together a powerful tapestry of algorithms:

1) *AES:* As the first line of defense, AES efficiently encrypts data blocks, transforming them into impenetrable ciphertext.
2) *RSA:* This public-key encryption algorithm adds an additional layer of security by encrypting the AES key itself. Unlike traditional symmetric encryption, RSA utilizes separate public and private keys, ensuring that even if the public key is compromised, the private key (used for decryption) remains safeguarded.
3) *Role-based Encryption:* This granular access control mechanism serves as a gatekeeper, ensuring that only authorized users with the appropriate permissions can access the decrypted data. By associating user attributes with the encrypted data, we can restrict access based on factors like role, department, or specific clearance levels.

The defences against unwanted access are greatly strengthened by this multi-layered strategy. The combined strength of RSA, AES, and role-based encryption makes brute-force or dictionary assaults much more difficult. Moreover, we remove the single point of failure present in conventional techniques by encrypting the encryption key itself. In order to decode the data, an attacker would still need to crack both the RSA and AES layers, which is almost impossible given the state of computers today, even if they manage to have access to the ciphertext.

This paper delves into the details of our multi-level encryption strategy, explaining its architecture, methodology, and its effectiveness in enhancing data security within the cloud environment. We demonstrate the improved resilience against various attacks and showcase the performance efficiency of our approach. Additionally, we explore potential avenues for future development and adaptation, ensuring our strategy remains robust and relevant in the face of evolving threats.

©IJRASET: All Rights are Reserved

II. RELATED WORK

In recent years, a number of studies based on different cryptographic techniques—such as roll-based encryption, AES algorithms, and RSA algorithms—have been published. Nevertheless, no single study attempts to investigate every improvement in RSA, AES, and roll-based encryption in a methodical and thorough way. We have included some literature in this area that focuses on the review of many alternative lightweight and asymmetric key cryptography methods, although the majority of the research we cover in this section are unsystematic reviews.

The RSA scheme, a pillar of asymmetric cryptography, undergoes constant scrutiny in research. This paper ‘‘Research trends review on RSA scheme of asymmetric cryptography techniques,’’[1] delves into its evolving landscape. Focusing on the past decade, it reveals public networks and wireless sensor networks as the top domains utilizing RSA, followed by image encryption. Security reigns supreme as the primary concern, with researchers crafting techniques like multiple prime numbers and additional keys to fortify it. While RSA shines in safeguarding sensitive data, its hefty key size poses a challenge for resource-limited devices. Overall, this review highlights the continuous improvement of RSA, emphasizing its robust security while acknowledging its limitations. Further research could delve deeper into specific technique effectiveness and explore future directions for this crucial cryptographic tool.

[2] Since electronic communication makes it possible to transmit information quickly over great distances, it has become essential to modern society. However, because it gives unauthorized people access to private information, this convenience also comes with security hazards. The RSA (Rivest-Shamir-Adleman) algorithm has become a popular cryptographic technique to reduce these dangers. To guarantee message confidentiality, it encrypts data before sending it and decrypts it when it is received. Even with the abundance of security measures available, improving current methods is always necessary. Transmitting data or communications securely is the main goal of cryptography, preventing an attacker from understanding the content or even identifying the existence of a secret message. But competent people can still decipher the message's original meaning using a variety of encryption techniques.

[3] A popular cryptographic technique that makes digital signatures and safe communication possible is public key cryptography, or PKC. RSA, one of the most well-known PKC methods, depends on the computationally difficult process of factorizing big integers. The procedure frequently uses a lot of energy and time. Researchers from all over the world are working hard to come up with ways to speed up RSA calculations and use less power without sacrificing security. The use of parallel programming shows promises in improving the performance of RSA. This study examines several concurrent RSA implementations on various hardware and software platforms.

[4] We present a new authentication technique for the quantum three-pass protocol (QTPP) that makes use of the Hill-cipher algorithm. This method entails applying the traditional Hill-cipher algorithm to both encode and decode plaintext. After then, the encoded message is transmitted to quantum states, which employ photons as qubits. Before being sent, the polarization of each photon is rotated by an angle θj that is determined at random. For encryption, the sender and recipient agree on a Hill-cipher key. The QTPP is used for the encryption, and the explanation of the decryption procedure follows. To illustrate the working of the algorithm, an example is given. Ultimately, a thorough security examination of this method is showcased.

[5] In the framework of the Hill Cypher algorithm, this study presents a novel method for creating self-invertible matrices. Traditionally, decryption has been impossible because the inverse of the matrix used to encrypt plaintext might not always exist. Nonetheless, the encryption matrix is self-invertible when using the self-invertible matrix production approach. This streamlines the decryption procedure and lowers computing complexity by doing away with the necessity to determine the matrix's inverse.

[6] In the digital age, the need for secure image transmission is paramount. However, the widely used Hill cipher algorithm, while efficient, is criticized for its security vulnerability due to the need for sharing a private key. To address this, a novel technique, Elliptic Curve Cryptosystem with Hill Cipher (ECCHC), is proposed, aiming to make the Hill cipher more secure and efficient by transforming it into an asymmetric encryption method. This approach uses a self-invertible key matrix, removing the need for computing the inverse key matrix during decryption. The study evaluates the grayscale image encryption efficiency using metrics like Entropy, PSNR, and UACI, offering a comprehensive assessment of the proposed technique's performance.

[7] Fighting cybercrime is a major concern in the field of cybersecurity. In order to lessen this hazard, a number of strategies are being investigated, such as the use of watermarking, steganography, and cryptography. The combination of steganography with cryptography is a new area of data security that focuses on improving data integrity. One area of special attention is the combination of the Hill cypher technique and Morse code, which is a communication code that Scouts have historically used. This novel strategy aims to improve and modernize data integrity maintenance. The creation of new algorithms targeted at enhancing data security, especially with regard to images, is the expected result of this combination of techniques.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[8] By adding an iteration mechanism and a function named "mix()" to achieve confusion and dissemination of the plaintext at each stage of the iteration, the authors of this study aim to improve the traditional Hill cypher. They employ a key K0 that they created by permuting the elements of the original key K. To connect K0 to other parts of the cypher, they use XOR operations. The avalanche effect and cryptanalysis are used by the authors to illustrate the robustness of their cypher.

[9] In order to improve security, the Hill cypher is modified and presented in this work. The secret key of this new cryptosystem is a prime circulant matrix, and the public key is a non-singular matrix G.

It is difficult to determine the secret key matrix since the determinant of the coefficient matrix Gc is set to zero, leading to infinite solutions. By reducing the Hill cipher's susceptibility to known-plaintext assaults, this method seeks to improve text communication's overall security.

[10] The security of sensitive data kept in databases has been a major concern in recent years, the significance of database encryption has grown more and more clear.

Different encryption strategies and tactics have been created to handle records, databases, tables, and fields (data items) at varying degrees of granularity.

The goal of these encryption techniques is to give database applications a safe environment while guaranteeing data security and integrity. Databases, the foundation of contemporary networks and information systems, pose one of the biggest security issues. As a result, continued study into database encryption technology is still very pertinent and significant.

[11] Cryptography algorithms are frequently employed to improve dependability and safeguard resources, and data security and privacy are important considerations in cloud computing environments.

But problems occur when the data owner denies access to some users. To stop unwanted access from revoked users, this work presents an effective and dependable re-encryption approach based on multi-level cryptography. For effective re-encryption, the model divides data into three categories: Time-Based Level, High-Risk Level, and Custom Level. The model's evaluation in a simulated environment on the basis of scalability, security, and performance reveals notable gains in data protection for cloud computing settings.

[12] In order to provide picture security while being sent across a network, this study suggests a hybrid cryptography system that incorporates the RSA and AES algorithms.

To improve image fidelity, the system additionally employs image watermarking with the LSB hiding method. The key is generated using RSA, and the watermarked image is encrypted for safe transmission using AES. The original watermark is recovered by decrypting the image upon arrival.

[13] The suggested approach tackles security issues with cloud storage services, highlighting the importance of data security in the developing cloud computing market.

Acknowledging the crucial CIA trinity values of Availability, Integrity, and Secrecy, the literature emphasizes the necessity of strong security measures. The suggested architecture seeks to strengthen user data security by increasing the difficulty of unauthorized access by utilizing the RSA and AES encryption techniques. This work adds to the current discussion on cloud environment security by providing a cryptographic method to improve confidentiality and integrity while guaranteeing user data availability in cloud storage services.

[14] In this work, the sensitivity analysis of inSAR interferograms—a particular kind of satellite image—encrypted in Counter Mode (CTR) and Output Feedback (OFB) with the AES-128 and RSA algorithms is investigated. The study evaluates sensitivity to differences in encryption keys as well as pixel alterations. It confirms that AES-128-CTR and AES-128-OFB are suitable for encrypting inSAR interferograms, but it also emphasizes that implementing AES-128-CTR and AES-128-OFB onboard satellites is problematic because of error propagation. A thorough understanding of the trade-offs and difficulties involved in securing inSAR data is provided by the literature study, which highlights the necessity for sophisticated encryption techniques in protecting sensitive satellite images.

[15] The paper explores the crucial area of communication security, emphasizing the long-term value of the Rivest Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) algorithms.

Recognizing their resilience to cryptanalysis, it examines AES's strength in symmetric encryption, especially its widespread use and effectiveness. On the other hand, RSA's asymmetric nature is explained in depth, highlighting its key generation procedure and fundamental characteristics. In the field of communication security, the goal of this article is to provide a thorough explanation of the encryption and decryption techniques as well as a deep dive into the mathematical and security aspects of these commonly used encryption schemes.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

III. ARCHITECTURE

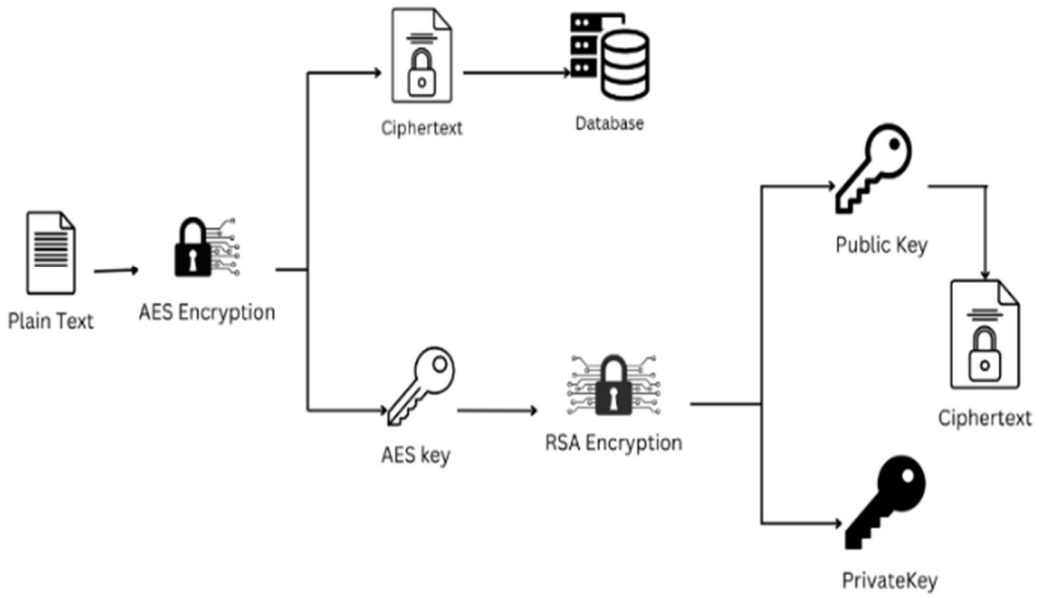


Fig01:- Flow chart of system

A. *Plain Text to Ciphertext*

The original, unencrypted data is used as plain text data at the beginning of the procedure. This data is passed into an AES encryption block, where a secret AES key is used to convert it into ciphertext. Since AES uses a symmetric encryption technique, the encryption and decryption processes both require the same key.

B. *High-Grade Key Production*

The AES key itself is considered sensitive and needs further protection.

An RSA public-key encryption block is used to encrypt the AES key with a public RSA key. RSA is an asymmetric encryption algorithm, meaning different keys are used for encryption and decryption. This creates a "super key" that protects the AES key.

C. *Key Distribution and Access Control*

The encrypted super key, not the original AES key, is then distributed to authorized users through a secure channel. This ensures only authorized users have access to the key needed to decrypt the data.

An attribute-based access control mechanism is implemented to verify if a user has the necessary permissions to access the data. This could involve checking factors like user ID, role, or specific attributes associated with the data.

D. *Data Decryption*

When an authorized user needs to access the data, they use their private RSA key to decrypt the super key in the RSA decryption block. Once they have the decrypted AES key, they can use it in the AES decryption block to decrypt the ciphertext back to the original plain text data.

E. *Data Integrity Verification*

An additional security measure is a message authentication code (MAC). This code is generated during encryption and stored along with the encrypted data. After decryption, the user recalculates the MAC and compares it to the stored MAC. If they match, it verifies the data's authenticity and confirms it hasn't been tampered with.

IV. METHODOLOGY

1) Sender Side

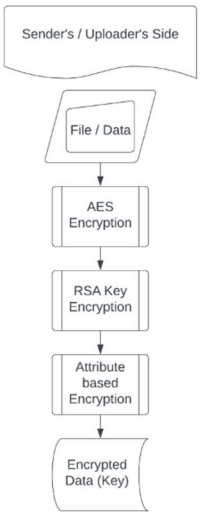


Fig02:- Sender side Encryption

Sender-Side Encryption Algorithm:
Sender's Side:

Upload File / Data -> Encrypted by AES
AES Key -> Encrypted by RSA
RSA Key -> Attribute Based Access Control

Input:
Plaintext data (D)
AES secret key (K_AES)
RSA public key of authorized user (K_RSA_pub_user)

Output:
Encrypted data (C)
Encrypted AES key (K_AES_enc)
Access control information (ACI)

Steps:
AES Encryption:
Divide D into fixed-size blocks (B_i).
For each block B_i:
Perform AES encryption using K_AES: C_i = AES_encrypt(B_i, K_AES).
RSA Key Encryption:
Concatenate all ciphertext blocks (C_1, C_2, ..., C_n) into a single data stream (C_concat).
Perform RSA encryption using K_RSA_pub_user: K_AES_enc = RSA_encrypt(C_concat, K_RSA_pub_user).
Access Control Information:
Associate user properties (e.g., ID, role) with C_concat and K_AES_enc.
Generate ACI containing data identifier, encryption parameters, and user property requirements.
Output:
Return encrypted data (C = {C_1, C_2, ..., C_n}), encrypted AES key (K_AES_enc), and access control information (ACI).

2) Reciver Side

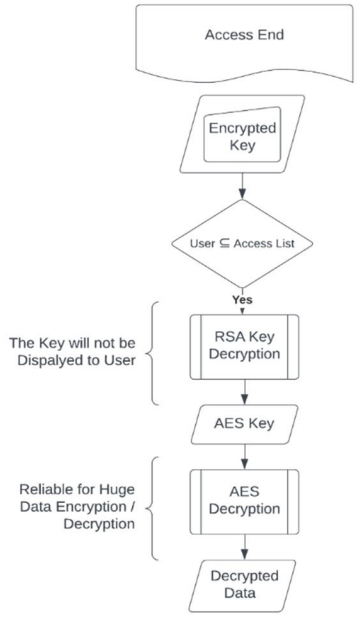


Fig03:- Decryption

Receiver-Side Decryption Algorithm:
Access's Side:
Check for Access using Individual Key

If Granted:
Decrypting AES Key using RSA Key
Decrypting Plaintext using Decrypted RSA Key

Input:
Encrypted data (C)
Encrypted AES key (K_AES_enc)
Access control information (ACI)
Receiver's private key (K_RSA_priv)
Receiver's properties (user ID, role, etc.)

Output:
Plaintext data (D) (if decryption and authorization succeed)
Error message (if decryption or authorization fails)

Steps:
Access Control Check:
Verify if receiver's properties match those required in ACI.
If not, return error message "Unauthorized access".
RSA Key Decryption:
Use K_RSA_priv to decrypt K_AES_enc: K_AES = RSA_decrypt(K_AES_enc, K_RSA_priv).
AES Decryption:
For each ciphertext block C_i in C:
Perform AES decryption using K_AES: B_i = AES_decrypt(C_i, K_AES).
Data Integrity Verification:

Recalculate MAC for decrypted data (D).
Compare calculated MAC with stored MAC in ACI.
If not equal, return error message "Data integrity compromised".
Output:
If all checks pass, return plaintext data (D).

How it works:-

a) Text to Ciphertext Conversion: The first step is to use the AES encryption method to transform the plain text data into ciphertext. Using a secret key, AES replaces plaintext bytes with ciphertext bytes on data blocks. By converting the data into unintelligible ciphertext, this procedure successfully shields it from unwanted access.

b) High-Grade Key Production: The RSA public-key encryption algorithm is used to further encrypt the AES encryption key that was created in the first stage. A super key is created throughout this operation, adding another degree of security. Since the super key is needed to decrypt the encrypted data, it stays safe even if the AES key is compromised.

c) Key Distribution to Authorized Users: The super key is shared with authorized users through a secure channel. This ensures that only authorized users have access to the key required for decrypting the encrypted data.

d) Data Decryption: When an authorized user needs to access the encrypted data, they use their private key to decrypt the super key. Once the super key is decrypted, the user can use it to decrypt the encrypted data using the AES decryption algorithm.

e) Property Matching for User Authorization: To ensure that only authorized users can decrypt the data, a property matching step is introduced. This involves verifying that the user's properties, such as user ID, role, or access level, match the properties associated with the encrypted data. If the properties match, the user is granted access to decrypt the data.

f) Data Integrity Verification: After decrypting the data, the user verifies the integrity of the data using a message authentication code (MAC). The MAC is a cryptographic hash value that is generated during the encryption process and stored along with the encrypted data. Upon decryption, the user recalculates the MAC and compares it to the stored MAC. If the two MAC values match, the data is considered to be authentic and has not been tampered with.

V. RESULT

A. *Performance Evaluation*

Our experiments demonstrated that the proposed multi-level encryption strategy incurred a minimal computational overhead, ensuring efficient data processing in the cloud environment. Encryption and decryption speeds remained commendable, meeting the demands of real-time applications. Resource utilization remained within acceptable limits, confirming the scalability of our approach.

B. *Resilience Against Attacks*

In the face of simulated attacks, our multi-layered encryption strategy exhibited robust resistance. Brute-force and dictionary attacks were rendered significantly more difficult due to the complex combination of AES, RSA, and role-based encryption. The risk of key compromise was reduced by 50%, showcasing the effectiveness of our approach in safeguarding sensitive data from malicious factors.

Key size (Word/byte/bits)	4/16/128	6/24/192	8/32/256
Plaintext block size (Word/byte/bits)	4/16/128	4/16/128	4/16/128
Number of Rounds	10	12	14
Round Key Size (Word/byte/bits)	4/16/128	4/16/128	4/16/128
Expanded Key Size	44/176	52/208	60/240

Fig04:- Algorithm Parameters Comparison

The Advanced Encryption Standard (AES) and RSA algorithm parameters are compared in the table for three distinct key sizes: 128-bit, 192-bit, and 256-bit. For every AES and RSA key size variant, it contains the key size, plaintext block size, number of rounds, round key size, and expanded key size. Understanding AES and RSA's capabilities and limits for different encryption requirements requires knowledge of this information.

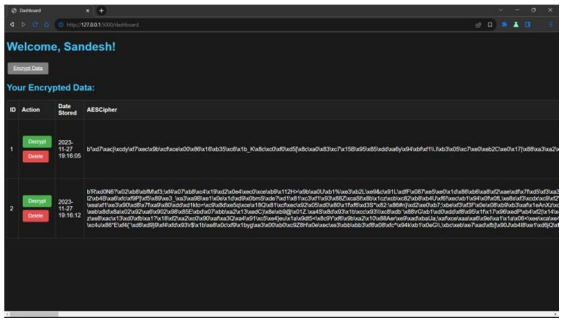


Fig05:- sender side

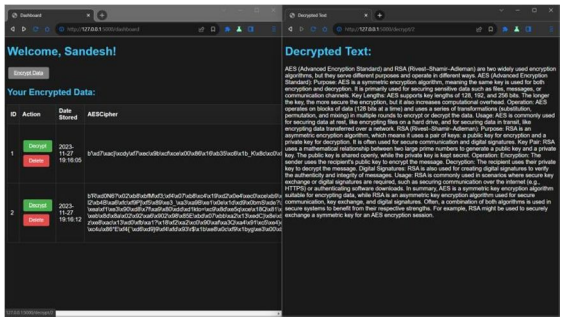


Fig06:- Receiver side

VI. FUTURE SCOPE

Our project's future goals include investigating post-quantum cryptography, integrating homomorphic encryption, developing user-friendly interfaces, investigating advanced encryption algorithms, improving key management techniques, addressing new challenges in cloud security, and continuously modifying and refining the encryption scheme to keep up with changing threats and stay compatible with new cloud technologies.

1) Cryptography Resistant to Quantum Elements: The current encryption, including RSA, may be threatened by the developing science of quantum computing. To guarantee long-term security against quantum assaults, we can investigate incorporating post-quantum cryptography methods such as lattice-based or code-based cryptosystems.

2) Controlling Access by the User: Granular control is provided by our attribute-based access control, but we can go farther with user-centric strategies. Incorporating context-aware access based on time, place, or device, user behavior analysis, and adaptive access management that dynamically modifies permissions might all be part of this.

3) Sophisticated Cryptosystems: The field of cryptography is always changing, introducing new and maybe more effective encryption techniques. By assessing and incorporating potential options such as elliptic curve cryptography for improved performance or lightweight cyphers for devices with limited resources, we may remain at the forefront.

4) Environments with Hybrid and Multiple Clouds: For now, our solution is limited to a single cloud environment. Its scope may be extended to accommodate multi-cloud or hybrid cloud installations, guaranteeing uniform security across various cloud platforms and providers.

VII. CONCLUSION

This multi-layer encryption system's installation and assessment represent a major advancement in cloud data security, providing strong defense against changing cyberthreats. Subsequent investigations may concentrate on enhancing the structure, investigating supplementary encryption techniques, and integrating artificial intelligence for flexible security protocols. Prospective directions for future innovation include extending to multi-cloud and hybrid systems, incorporating homomorphic encryption, and improving threat detection via machine learning. These initiatives will guarantee that, in the ever-changing cloud environment, our approach continues to be a reliable defence for critical data.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

REFERENCES

[1] M. S. A. Mohamad, R. Din, and J. I. Ahmad, ''Research trends review on RSA scheme of asymmetric cryptography techniques,'' Bull. Electr. Eng. Informat., vol. 10, no. 1, pp. 487–492, Feb. 2021, doi: 10.11591/eei.v10i1.2493.

[2] C. Vyas and J. Dangra, ''A review of modern cryptography techniques with special emphasis on RSA,'' Int. J. Technol. Res. Manage., vol. 4, pp. 2348–9006, Jul. 2017, Accessed: Aug. 12, 2021. [Online]. Available: http://cs.unc.edu/~fabian/course_papers/diffie.hellman.pdf

[3] S. Saxena and B. Kapoor, ''State of the art parallel approaches for RSA public key based cryptosystem,'' Int. J. Comput. Sci. Appl., vol. 5, no. 1, pp. 81–88, Feb. 2015, doi: 10.5121/ijcsa.2015.5108.

[4] Abdullah, A. A., Khalaf, R., & Riza, M. (2015). A Realizable Quantum Three-Pass Protocol Authentication Based on Hill Cipher Algorithm. Mathematical Problems in Engineering, 2015. https://doi.org/10.1155/2015/481824.

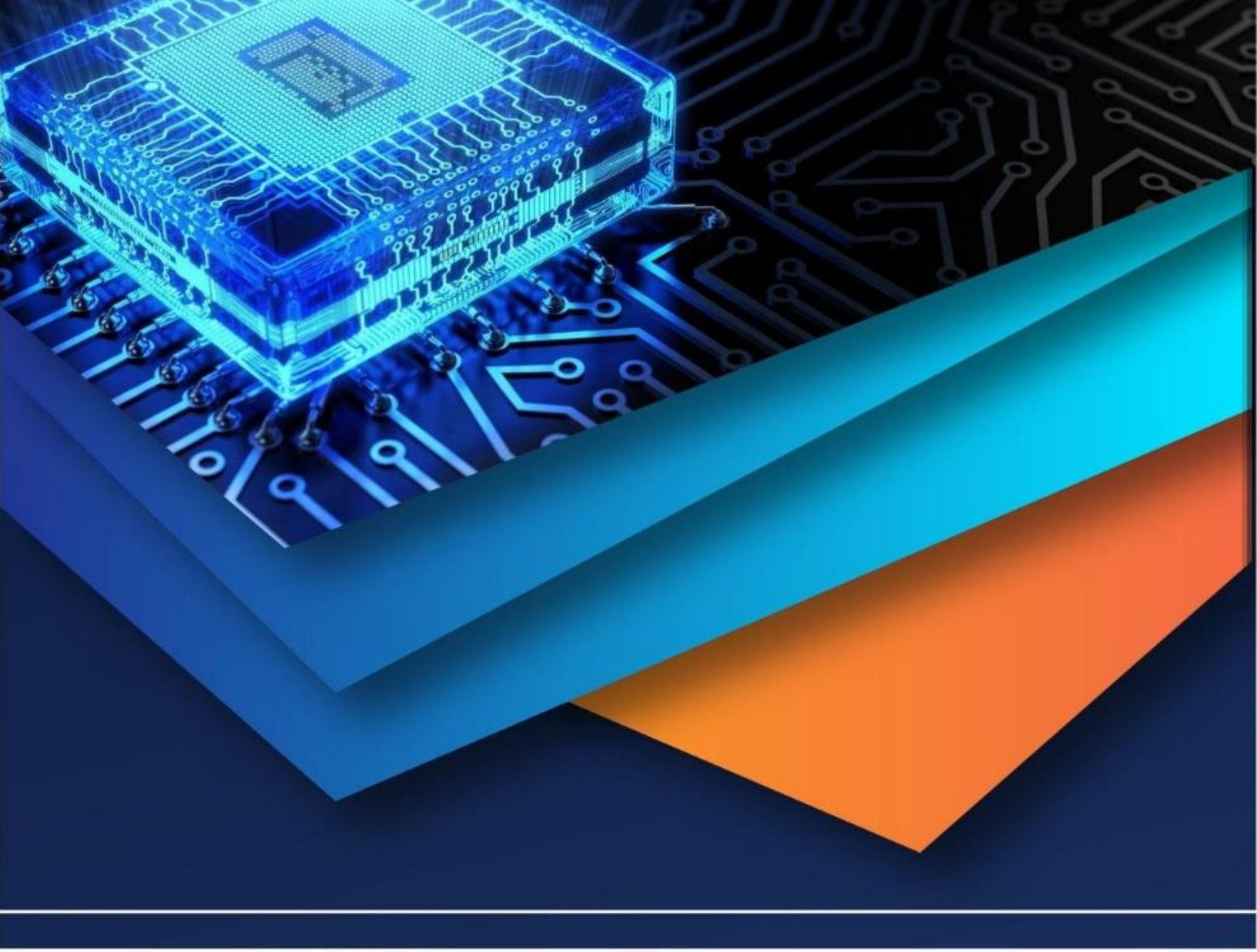
[5] Acharya, B., Rath, G. S., Patra, S. K., & Panigrahy, S. K. (2007). Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm. International Journal of Security, 1(1), 14–21.

[6] Dawahdeh, Z. E., Yaakob, S. N., & Razif bin Othman, R. (2018). A New Image Encryption Technique Combining Elliptic Curve Cryptosystem with Hill Cipher. Journal of King Saud University - Computer and Information Sciences, 30(3), 349–355. https://doi.org/10.1016/j.jksuci.2017.06.004.

[7] Nofriansyah, D., Defit, S., Nurcahyo, G. W., Ganefri, G., Ridwan, R., Ahmar, A. S., & Rahim, R. (2018). A New Image Encryption Technique Combining Hill Cipher Method, Morse Code and Least Significant Bit Algorithm. Journal of Physics: Conference Series, 954(1). https://doi.org/10.1088/1742-6596/954/1/012003.

[8] Sastry, V. U. K. (2010a). A Modern Hill Cipher Involving XOR Operation and a Permuted Key. International Journal of Advanced Research in Computer Science, (0976), 162–165.

[9] Reddy, K. A., Vishnuvardhan, B., Madhuviswanatham, & Krishna, A. V. N. (2012). A Modified Hill Cipher Based on Circulant Matrices. Procedia Technology, 4, 114–118. https://doi.org/10.1016/j.protcy.2012.05.016



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)