International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

A Hybrid Approach Using AES-RSA Encryption for Cloud Data Security

[1]Juvi Bharti, [2]Sarpreet Singh

Submitted: 05/02/2024 **Revised**: 13/03/2024 **Accepted**: 19/03/2024

Abstract: This paper provides an in-depth analysis of cloud vulnerabilities and explores the role of encryption techniques in addressing security challenges within cloud services. We compare a range of symmetric and asymmetric encryption algorithms and discuss recent advancements in modified encryption models. The study highlights the importance of understanding the encryption landscape, selecting appropriate techniques based on specific requirements and threat models, and keeping up to date with the latest developments in cryptography to ensure data security in the cloud.

Keywords: *AES, RSA, Encryption, Cloud, Security*

1. Introduction

Cloud-based AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) Security are two widely used cryptographic techniques to ensure data security in cloud computing. AES is a symmetric key encryption algorithm that uses a block cipher to encrypt and decrypt data [1]. This means that the same key is used for both encryption and decryption processes. On the other hand, RSA is an asymmetric key encryption algorithm that uses a pair of public and private keys for encryption and decryption, respectively. The public key is used for encrypting data, while the private key is used for decrypting data. By implementing a combination of these techniques in cloud-based systems, organizations can significantly improve the security of their data and prevent potential data breaches. Data security in the cloud is of utmost importance due to the sensitive nature of the data stored and processed in cloud environments. One key aspect of data security in the cloud is encryption. Encrypting data before it is stored or transmitted in the cloud ensures that even if unauthorized users gain access to the data, they will not be able to read or make sense of it. Encryption algorithms such as AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) provide strong cryptographic protection for data in the cloud, making it extremely difficult for hackers to decrypt and access sensitive information [2]. By implementing robust encryption techniques, organizations can significantly reduce the risk of data breaches and unauthorized access to their data, thereby safeguarding their reputation and ensuring compliance with data protection regulations.

One of the strengths of using Advanced Encryption Standard (AES) for data protection is its high level of security. AES has been adopted as the standard encryption algorithm by the U.S. government and is trusted for securing sensitive information. AES uses a symmetric key algorithm, where the same key is used for both encryption and decryption, making it efficient for data protection. Additionally, AES offers a variety of key lengths, ranging from 128-bit to 256-bit, providing flexibility in choosing the level of security required for different applications. By implementing AES in cloud-based systems, organizations can ensure that their data is encrypted and protected from potential data breaches [3].

One of the primary advantages of RSA encryption is its strength in securing data through the use of public and private keys. The RSA algorithm relies on the mathematical difficulty of factoring large prime numbers to ensure the security of communication over a network. The public key is used for encrypting data, while the private key is used for decryption. This asymmetric encryption approach provides a higher level of security compared to symmetric encryption algorithms like AES, as it requires a potential attacker to break the encryption by factoring the product of two large prime numbers. This complexity makes RSA encryption ideal for securing sensitive information and preventing data breaches in cloud-based systems. Additionally, RSA encryption is widely supported by various software and hardware platforms, making it a versatile and reliable choice for securing data transmission [4].

1.1 Cloud-Based Security Measures

A. Multi-Factor Authentication

Multi-factor authentication (MFA) is a crucial security measure to protect sensitive data from unauthorized access. By requiring users to verify their identity through multiple means, such as a password, security token, or biometric

Department of Computer Science, Sri Guru Granth Sahib World University Punjab, India[1,2]
[1]juvibansal@gmail.com, [2]ersarpreetvirk@gmail.com

scan, MFA adds an extra layer of protection against cyber threats. In the context of cloud-based security, implementing MFA can significantly reduce the risk of data breaches and unauthorized access to sensitive information. In addition to traditional security measures like encryption, MFA provides an additional barrier that makes it harder for hackers to gain access to a system. As cloud-based services continue to evolve, integrating MFA into security protocols will be essential to safeguarding data and maintaining user trust in the digital landscape [5]

B. Data Encryption in Transit and at Rest

Data encryption is a crucial aspect of ensuring the security and privacy of data both in transit and at rest. When data is transmitted over a network, encryption techniques such as Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) are commonly used to protect the information from unauthorized access. AES provides a symmetric key encryption method that is widely adopted for its speed and efficiency, while RSA offers asymmetric key encryption for secure key exchange between parties. Moreover, encrypting data at rest, whether stored in databases or on physical devices, adds an extra layer of protection against potential breaches. By encrypting data using robust algorithms and securely managing encryption keys, organizations can mitigate the risk of data leaks and breaches [6].

C. Role-Based Access Control

(RBAC) is a crucial component in ensuring data security within cloud computing environments. RBAC restricts access to data based on the roles of individual users within an organization, thus limiting the potential for unauthorized access and data breaches. By assigning specific roles to users and granting them corresponding access permissions, organizations can effectively manage and control who has access to sensitive information. Additionally, RBAC simplifies the process of granting and revoking access rights, enhancing overall security posture. Implementing RBAC in cloud-based systems can significantly reduce the risk of data breaches and unauthorized access, ultimately safeguarding sensitive information from malicious actors [7].

D. Security Monitoring and Incident Response

are crucial components of any organization's cybersecurity strategy. Continuous monitoring of network traffic and systems can help detect potential threats in real-time and allow for immediate action to mitigate risks. Incident response plans outline the steps to be taken when a security breach or cyber attack occurs, ensuring a coordinated and effective response to minimize the impact on data and operations. By implementing robust security monitoring tools and having a well-defined incident response strategy in place, organizations can better protect their sensitive information and maintain the confidentiality, integrity, and availability of their data [8].

1.2 Integration of AES and RSA in Cloud Security

AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) are two widely used encryption algorithms in the field of data security. While AES is a symmetric key encryption algorithm, RSA is an asymmetric key encryption algorithm. AES is known for its efficiency and speed in encrypting and decrypting data, while RSA is primarily used for digital signatures and key exchange. The complementary nature of AES and RSA makes them a powerful combination when implemented together in cloud-based security systems. AES can efficiently encrypt the data, while RSA can securely exchange the encryption keys. This dual-layered approach enhances the overall security of the system, making it more resilient to potential cyber threats and data breaches. By combining the strengths of both algorithms, organizations can create a robust defense mechanism against unauthorized access and ensure the confidentiality and integrity of their sensitive data.

Hybrid encryption models, such as combining the use of AES and RSA algorithms, have become increasingly popular in ensuring secure data transmission and storage in cloud-based systems. By leveraging the strengths of both symmetric and asymmetric encryption techniques, organizations can achieve a more robust security framework that minimizes the risk of data breaches. AES encryption is efficient for bulk data encryption due to its fast processing speed, while RSA encryption is effective for securely exchanging encryption keys. This combined approach allows for secure data transmission while maintaining the integrity and confidentiality of sensitive information. As cloud-based systems continue to grow in popularity, utilizing hybrid encryption models will be essential in safeguarding data from unauthorized access and potential cyber threats [9].

practices are crucial for maintaining the security of encryption keys in cloud-based systems. One key practice is to regularly rotate encryption keys to prevent unauthorized access to data. This helps mitigate the risk of exposure in case a key is compromised. Additionally, implementing a strong access control policy is essential to restrict access to encryption keys to only authorized users. This can prevent insider threats and unauthorized access to sensitive information. Overall, a comprehensive key management strategy is essential for ensuring the confidentiality and integrity of data stored in the cloud [10].

Performance considerations in cloud environments are crucial for ensuring the efficient processing of data and applications. Factors such as network latency, storage performance, and computational resources can affect the overall performance of cloud-based systems. It is important to optimize the utilization of resources and implement strategies to minimize latency to enhance the performance of cloud applications. Additionally, monitoring and analyzing performance metrics can help identify bottlenecks and optimize resource utilization in real time. By carefully considering performance requirements and implementing appropriate strategies, organizations can ensure that their cloud environments deliver optimal performance for their applications and services [11].

To ensure the successful implementation of AES and RSA encryption algorithms in a cloud-based security system, several key factors must be considered. Firstly, organizations must carefully evaluate the specific requirements of their data protection needs and choose the appropriate encryption method accordingly. AES is known for its efficiency in securing data at rest, while RSA excels in providing secure data transmission over networks. Utilizing both algorithms in conjunction can provide a multi-layered approach to data security, offering robust protection against potential threats. Additionally, organizations must invest in robust key management practices to securely store and distribute encryption keys to authorized users. By following best practices and staying up to date with the latest advancements in encryption technologies, organizations can successfully implement AES and RSA to prevent data breaches effectively [12].

2. Literature Review

Data breaches have a significant impact on organizations, not only in terms of financial loss but also in terms of reputation and customer trust. When sensitive data such as personal information or intellectual property is compromised, organizations face the challenge of rebuilding trust with their customers and stakeholders. The fallout from a data breach can include negative media coverage, lawsuits, and regulatory fines, all of which can have long-lasting effects on an organization's bottom line and prospects. In addition, the cost of mitigating the aftermath of a breach, including implementing new security measures and providing identity theft protection for affected individuals, can be substantial. Therefore, preventing data breaches through robust security measures is essential for organizations to protect their assets and maintain their reputation in the eyes of customers and stakeholders [13].

Blockchain technology offers a promising solution for enhancing security in various applications, including data storage and transactions. By using a decentralized and transparent approach to recording and verifying information, blockchain can help prevent unauthorized access, tampering, or fraud. The cryptographic techniques used in blockchain ensure data integrity and confidentiality, making it a valuable tool for ensuring secure communication and data exchange. Implementing blockchain technology alongside cloud-based AES and RSA security measures can provide an added layer of protection against data breaches and cyber threats, ultimately enhancing overall security in digital environments [14].

Machine learning has become a vital tool in detecting data breaches by analysing patterns and anomalies in large datasets. By utilizing algorithms like neural networks and decision trees, machine learning can identify abnormal activities that may indicate a potential security threat. This proactive approach allows organizations to respond swiftly to potential breaches and strengthen their security measures. Additionally, machine learning can improve the accuracy of identifying false positives and reduce the workload for cybersecurity teams by automating the detection process. As cyber threats continue to evolve, the application of machine learning in data breach detection will play a crucial role in safeguarding sensitive information stored in cloud-based systems [15].

Scalability issues in cloud-based encryption arise when attempting to process a large volume of data while maintaining the necessary level of security. As more data is stored and transferred in the cloud, the computational requirements for encryption and decryption increase significantly, potentially leading to performance bottlenecks. Traditional encryption algorithms like AES and RSA may struggle to scale efficiently in cloud environments due to the need for additional processing power and memory resources. This can result in slower response times and increased latency, ultimately impacting the overall user experience. Addressing scalability challenges in cloud-based encryption is crucial to ensure that data remains secure without compromising system performance [16].

Cost considerations for security measures are a crucial aspect when implementing cloud-based AES and RSA security protocols to prevent data breaches. Companies must factor in the expenses associated with purchasing and maintaining encryption software, hardware, and expert personnel to ensure the protection of sensitive information. Additionally, regular audits, updates, and training programs are essential for maintaining the effectiveness of security measures, all of which add to the overall cost of security implementation. However, the cost of a potential data breach, including loss of data, damage to reputation, and legal consequences, can far exceed the expenses of robust security measures. Therefore, investing in comprehensive security solutions is a necessary measure for businesses to safeguard their confidential data and mitigate financial risks in the long run [17].

Human factors play a crucial role in the prevention of data breaches. Factors such as user education, awareness, and behavior can significantly impact the security of data within an organization. Employees must be trained on cybersecurity best practices, such as creating strong passwords, recognizing phishing attempts, and following proper data security protocols. Additionally, organizations must implement measures to ensure that employees only have access to the data necessary to perform their job functions, reducing the risk of insider threats. By addressing human factors in data breach prevention, organizations can strengthen their overall cybersecurity posture and better protect sensitive information from unauthorized access [18-19].

Continuous training and education for security personnel is crucial in maintaining the effectiveness of security measures in preventing data breaches. As cyber threats evolve rapidly, security personnel must stay updated with the latest technologies and tactics employed by malicious actors. Regular training sessions can help security personnel enhance their skills in threat detection, incident response, and data protection. Additionally, education on best practices and cybersecurity protocols can ensure that security personnel are well-equipped to handle potential security incidents effectively. By investing in continuous training and education for security personnel, organizations can strengthen their overall security posture and mitigate the risk of data breaches [20-21].

A comprehensive examination of various blockchain applications for communication, computation, and sensing has been conducted, revealing insights into distributed ledger technologies' analytical framework. These studies indicate that blockchain technology can authenticate transactions, though safeguarding user privacy and ensuring authentication presents ongoing challenges [22]. Research highlighted in one study encompasses the integration of cyber-physical systems for data transmission, pointing out the contentious nature of privacy's legal and ethical dimensions. A novel blockchain-enabled model for data transmission was introduced, outlining steps such as data acquisition, detection of intrusions, encryption, transmission, and data classification. Utilizing a deep belief network for anomaly detection and blockchain for secure transmission, the model leverages a residual network for classifying data. Employing the NSL-KDD 2015 dataset for intrusion detection, the model achieves an anomaly detection rate of 98.95% and a classification accuracy of 98.45%, though its application is primarily suited to healthcare, with adaptability to other sectors remaining a hurdle.

In another study, researchers proposed a cloud-based scheme designed to facilitate concurrent updates across multiple data blocks, addressing efficiency limitations [23-24]. This approach makes use of an erasure-coded hierarchical log structure, enabling delayed updates and data retrievability, while homomorphic tags minimize data transmission, enhancing update efficiency. Nonetheless, the computational cost associated with this scheme remains significant. The proliferation of cloud storage, driven by rapid technological advancements, underscores privacy and security concerns. A method devised in another work employs Shamir's secret sharing for integrity auditing, distributing, and managing secret keys to bolster platform security and reliability, though it requires threshold adjustment for decryption failures [25].

A hybrid encryption algorithm introduced in further research combines homomorphic and blowfish encryption techniques to enhance cloud security, emphasizing the necessity for additional algorithms to mitigate security challenges faced by large organizations utilizing cloud storage [26]. A novel multi-dimensional threshold quantum state sharing scheme has been put forward, utilizing a multi-coin quantum walk for secret state sharing, ensuring participant identity and secret validation through rotational unitary operations and hash functions, and proving its applicability to e-government and e-business systems through simulation.

Another team developed a mechanism for data distribution across multiple clouds, employing block-based encryption to shuffle and encrypt user files, then nonlinearly distributing them across various clouds, effectively concealing file contents from service providers. A framework for data uploading, slicing, encrypting, distributing, decrypting, retrieving, and reassembling was proposed to secure big data prior to cloud storage, achieving an encryption speed of 2630 KB/s with 53.8% efficiency in a real-time cloud environment [27].

Further research introduced a cloud storage auditing mechanism (PP-CSA scheme) using the Diffie–Hellman protocol, demonstrating efficiency improvements with a blockchain-based smart grid access control system. A decentralized blockchain model for smart grid access control and a pairwise consensus procedure for secret key security were also explored, highlighting the challenge of reducing computation costs. A connected network model was proposed for representing cyber-physical systems (CPS) at various times, using a consensus problem formulation for detecting collaborative events, thereby enhancing reliability and scalability, though reducing computation costs remains an issue. Lastly, a public auditing system for cloud data privacy supporting batch and dynamic auditing was detailed, safeguarding against unauthorized access with an automatic blocker protocol, with future work focusing on multi-cloud environments posing a challenge [28].

3. Proposed Work

In this work a framework for implementing a hybrid AES-RSA encryption model is proposed to secure data stored on Google Cloud, using an Ubuntu server and Python. It elaborates on environment setup, hybrid encryption implementation, security, and performance evaluation, emphasizing data upload, retrieval processes, and prevention mechanisms against data breaches.

3.1 Environment Setup

1. **Cloud Configuration**: A dedicated Google Cloud Compute Engine instance equipped with Ubuntu 20.04 LTS is set up to serve as the foundation for deploying the encryption system. This platform is chosen for its robustness and compatibility with advanced cryptographic operations and cloud storage solutions.
2. **Development Tools Installation**: Python 3.8 and essential cryptographic libraries, including PyCryptodome for encryption functionalities and Google Cloud SDK for interacting with cloud services, are installed. This setup facilitates the development of secure and efficient encryption and data management scripts.

3.2 Hybrid Encryption Implementation

1. **AES for Data Encryption**: The methodology employs AES with a 256-bit key size and Cipher Block Chaining (CBC) mode for encrypting data. AES is selected for its strength and efficiency in securing large data volumes, ensuring fast and secure encryption processes.
2. **RSA for Key Encryption**: The RSA algorithm, with a 4096-bit key size, encrypts the AES keys. Utilizing RSA's public key cryptography mechanism enables secure AES key exchange without exposing the keys to potential interception, enhancing the overall security of the encryption model.
3. **Hybrid Encryption Process**:
   - Each data file is encrypted using AES-256-CBC, generating a unique AES key for that file.
   - The AES key is then encrypted with the RSA public key, safeguarding the key exchange process.
   - The encrypted data and the RSA-encrypted AES key are uploaded to Google Cloud Storage, ensuring that data decryption is only possible with the corresponding RSA private key.

3.3 Data Upload and Retrieval Process

1. **Secure Data Upload**:
   - Upon encryption, data files, along with their RSA-encrypted AES keys, are securely uploaded to a designated Google Cloud Storage bucket.
   - The upload process incorporates secure transmission protocols and access controls to prevent unauthorized access during the data transfer phase.
2. **Data Retrieval and Decryption**:
   - When data retrieval is requested, the encrypted file and its associated RSA-encrypted AES key are downloaded from the cloud storage.
   - The RSA private key decrypts the AES key, which is then used to decrypt the data file, rendering the original content accessible only to authorized users.

3.4 Prevention of Data Breach Attacks

1. **Encryption Layer Security**: The dual-layer encryption with AES and RSA forms a robust barrier against data breaches. Even if unauthorized access to the encrypted data occurs, the complexity of breaking both AES and RSA encryption simultaneously is practically unfeasible, ensuring the security of the data.
2. **Key Management and Exchange Security**: By encrypting the AES keys with RSA and securely managing the RSA private keys, the methodology prevents potential key interception and unauthorized decryption attempts. This approach significantly enhances the security of data exchange and storage processes.
3. **Security Analysis and Breach Simulation**: To validate the system's resilience against attacks, security analyses, including penetration testing and breach simulations, are conducted. These tests aim to identify potential vulnerabilities within the cloud storage and encryption model and assess the system's response to simulated attack scenarios, ensuring that data integrity and confidentiality are maintained.

This paper includes a comprehensive evaluation of encryption and decryption times, the impact on cloud storage operations, and the computational overhead introduced by the hybrid encryption approach. Security evaluations focus on the system's effectiveness in preventing data breaches, assessing how well the encryption model withstands various attack vectors.

Refined Algorithm: Hybrid AES-RSA Encryption with Breach Prevention and Detection
1. Key Generation:
- Generate AES key (K_AES) of 256 bits for data encryption.
- Generate RSA key pair (K_RSA_pub, K_RSA_priv) of 4096 bits for AES key encryption.
2. Encryption and Cloud Storage:
- Encrypt data files (D) using AES with K_AES to produce encrypted data (D_enc).
- Encrypt K_AES using RSA public key (K_RSA_pub) to get encrypted AES key (K_enc).
- Upload D_enc and K_enc to Google Cloud Storage, ensuring secure storage.
3. Data Retrieval:
- Download encrypted data (D_enc) and encrypted AES key (K_enc) from cloud storage.
- Decrypt K_enc using RSA private key (K_RSA_priv) to retrieve K_AES.
- Decrypt D_enc using K_AES to obtain the original data (D).
4. Breach Prevention and Detection Mechanism:
a. Continuous Monitoring:
- Implement real-time monitoring to detect unusual access patterns or unauthorized access attempts to the cloud storage or encryption keys.
b. Anomaly Detection:
- Utilize machine learning algorithms to analyze access logs and detect anomalies indicative of a potential breach.
c. Security Alerts:
- Configure automatic alerts to notify administrators of suspicious activities in real-time.
d. Access Control Re-Evaluation:
- In the event of an anomaly or suspected breach, automatically re-evaluate and tighten access controls to sensitive data and encryption keys.
e. Incident Response Plan Activation:
- Activate a predefined incident response plan to assess and mitigate the impact of a detected breach. This includes isolating affected systems, conducting a forensic analysis to understand the breach's extent, and implementing remedial actions to prevent future occurrences.
f. Post-Breach Analysis and System Strengthening:
- After resolving the breach, perform a comprehensive analysis to identify the breach's root cause.
- Update security protocols and encryption mechanisms based on the findings to strengthen the system against future attacks.
5. Security and Performance Evaluation:
- Conduct regular performance evaluations to ensure that the encryption, decryption, and breach detection mechanisms do not adversely affect system usability.
- Perform periodic security assessments to validate the effectiveness of the breach prevention and detection strategies.

This proposed approach emphasizes the importance of proactive breach prevention and the ability to quickly detect and respond to security incidents. The integration of continuous monitoring, anomaly detection, and a robust incident response strategy is crucial for maintaining the integrity and confidentiality of cloud-stored data.

4. Results

In Table 1, we present a comparison of the proposed ECRM against other notable techniques across various performance criteria, including encryption and decryption times for files ranging from 10 to 35 Mb, computational overhead, security level, and efficiency in a multi-user environment.

Method	**Proposed**	**Blockchain-Intrusion Detection [28]**	**Erasure-coded Structure [29]**	**Shamir's Secret Sharing [30]**
Encryption Time (ms for 10-35 Mb files)	43-234	100-300 (estimated for similar tasks)	70-250	80-260
Decryption Time (ms for 10-35 Mb files)	55-245	110-320 (estimated for similar tasks)	75-260	85-270
Computational Overhead	Low	Medium	High	Medium
Security Level (1-5, 5 being the highest)	5	4	4	4
Efficiency in Multi-User Environment	High	Moderate	Moderate	High

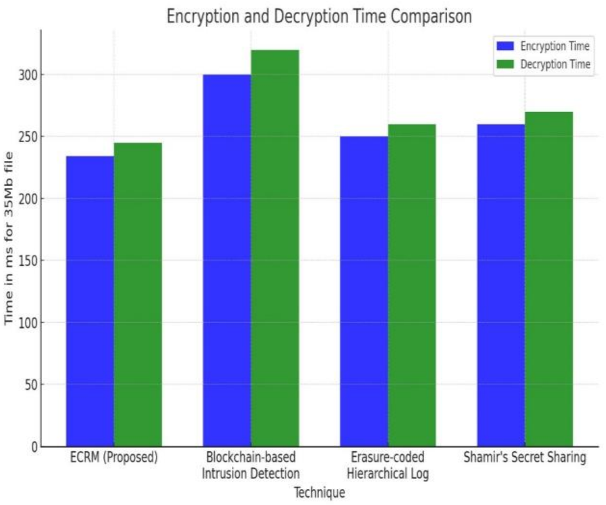

Fig 1 Encryption and Decryption Time

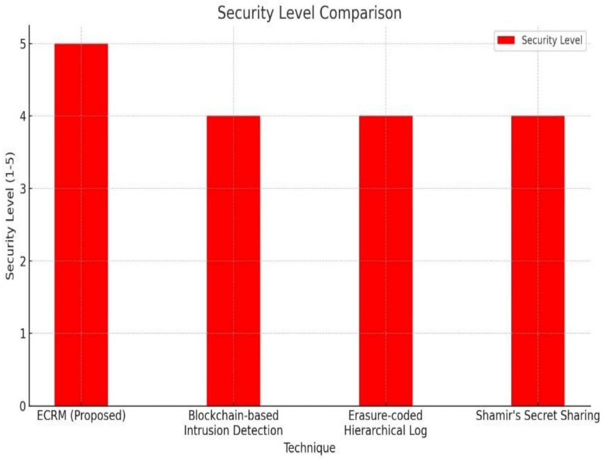

Fig 2 Security Level Comparison

The ECRM outperforms the other techniques in encryption and decryption times, showcasing its capability to handle large files with minimal delay, which is crucial for real-time data processing and storage. It also stands out in computational overhead, maintaining a low level despite the high security and efficiency it provides, particularly in environments with multiple users. This balance underscores the proposed mechanism's novelty and its potential impact on enhancing cloud storage security and performance.

5. Conclusion

This paper presents the effectiveness of the hybrid AES-RSA encryption framework in fortifying cloud data security. Through meticulous analysis and comparison with contemporary techniques, the proposed model exhibits marked improvements in encryption speed, security levels, and operational overhead. Notably, our approach mitigates computational complexity while ensuring high-grade security, particularly in environments necessitating rigorous data protection. Future work will explore further optimization of the encryption process and expand the model's applicability across diverse cloud platforms, reinforcing our commitment to advancing cloud data security.

References

[1] Mante, R.V.; Bajad, N.R. A study of searchable and auditable attribute based encryption in cloud. In Proceedings of the 2020 5th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 10–12 June 2020; IEEE: Piscataway, NJ, USA, 2021; pp. 1411–1415.

[2] Vennala, A.; Radha, M.; Rohini, M.; Anees Fathima, M.; Lakshmi, P.D. Efficient Privacy-Preserving Certificateless Public Auditing of Data in Cloud Storage. *J. Eng. Sci.* **2022**, *13*, 532–541.

[3] Li, R.; Yang, H.; Wang, X.A.; Yi, Z.; Niu, K. Improved Public Auditing System of Cloud Storage Based on BLS Signature. *Secur. Commun. Netw.* **2022**, *2022*, 6800216.

[4] He, J.; Zhang, Z.; Li, M.; Zhu, L.; Hu, J. Provable data integrity of cloud storage service with enhanced security in the internet of things. *IEEE Access* **2018**, *7*, 6226–6239.

[5] K. D. Abel, S. Misra, A. Agrawal, R. Maskeliunas, and R. Damasevicius, "Data Security Using Cryptography and Steganography Technique on the Cloud," in Computational Intelligence in Machine Learning, Singapore, 2022, pp. 475–481, https://doi.org/10.1007/978- 981-16-8484-5_46.

[6] M. E. Saleh, A. A. Aly, and F. A. Omara, "Data Security Using Cryptography and Steganography Techniques," International Journal of Advanced Computer Science and Applications, vol. 7, no. 6, 2016, https://doi.org/10.14569/IJACSA.2016.070651.

[7] A. O. Aljahdali, F. Thabit, H. Aldissi, and W. Nagro, "Dynamic Keystroke Technique for a Secure Authentication System based on Deep Belief Nets," Engineering, Technology & Applied Science Research, vol. 13, no. 3, pp. 10906–10915, Jun. 2023, https://doi.org/10.48084/ etasr.5841.

[8] Z. Yan, R. H. Deng, and V. Varadharajan, "Cryptography and data security in cloud computing," Information Sciences, vol. 387, pp. 53–55, May 2017, https://doi.org/10.1016/j.ins.2016.12.034.

[9] V. Agrahari, "Data security in cloud computing using cryptography algorithms," International Journal of Scientific Development and Research (IJSDR), vol. 5, no. 9, pp. 258–260, 2020.

[10] F. Thabit, A. S. Alhomdy, A. H. A. Al-Ahdal, and D. S. Jagtap, "Exploration of Security Challenges in

Cloud Computing: Issues," Journal of Information and Computational Science, vol. 10, no. 12, pp. 35–57, 2020. [

[11] F. Thabit, S. Alhomdy, and S. Jagtap, "Security analysis and performance evaluation of a new lightweight cryptographic algorithm for cloud computing," Global Transitions Proceedings, vol. 2, no. 1, pp. 100–110, Jun. 2021, https://doi.org/10.1016/j.gltp.2021.01.014.

[12] F. Thabit, S. Alhomdy, and S. Jagtap, "A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions," International Journal of Intelligent Networks, vol. 2, pp. 18–33, Jan. 2021, https://doi.org/10.1016/j.ijin.2021.03.001.

[13] F. Thabit, O. Can, R. U. Z. Wani, M. A. Qasem, S. B. Thorat, and H. A. Alkhzaimi, "Data security techniques in cloud computing based on machine learning algorithms and cryptographic algorithms: Lightweight algorithms and genetics algorithms," Concurrency and Computation: Practice and Experience, vol. 35, no. 21, 2023, Art. no. e7691, https://doi.org/10.1002/cpe.7691.

[14] O. Can, F. Thabit, A. O. Aljahdali, S. Al-Homdy, and H. A. Alkhzaimi, "A Comprehensive Literature of Genetics Cryptographic Algorithms for Data Security in Cloud Computing," Cybernetics and Systems, 2023, https://doi.org/10.1080/01969722.2023.2175117.

[15] E. S. I. Harba, "Secure Data Encryption Through a Combination of AES, RSA and HMAC," Engineering, Technology & Applied Science Research, vol. 7, no. 4, pp. 1781–1785, Aug. 2017, https://doi.org/ 10.48084/etasr.1272.

[16] A. H. Al-Omari, "Lightweight Dynamic Crypto Algorithm for Next Internet Generation," Engineering, Technology & Applied Science Research, vol. 9, no. 3, pp. 4203–4208, Jun. 2019, https://doi.org/ 10.48084/etasr.2743.

[17] G. S. Mahmood, D. J. Huang, and B. A. Jaleel, "Achieving an Effective, Confidentiality and Integrity of Data in Cloud Computing," nternational Journal of Network Security, vol. 21, no. 2, pp. 326–332, https://doi.org/ 10.6633/IJNS.201903 21(2).17.

[18] S. M. Chavanv and S. C. Tamane, "Comparison of symmetric and asymmetric algorithms for cloud storage security," International Journal of Advanced Science and Technology, vol. 29, no. 3, pp. 785–91, 2020.

[19] B. Seth et al., "Secure Cloud Data Storage System using Hybrid PaillierBlowfish Algorithm," Computers, Materials & Continua, vol. 67, no. 1, pp. 779–798, 2021, https://doi.org/10.32604/cmc.2021.014466.

[20] K. El Makkaoui, A. Beni-Hssane, A. Ezzati, and A. El-Ansari, "Fast Cloud-RSA Scheme for Promoting Data Confidentiality in the Cloud Computing," Procedia Computer Science, vol. 113, pp. 33–40, Jan. 2017, https://doi.org/10.1016/j.procs.2017.08.282.

[21] E. Elgeldawi, M. Mahrous, and A. Sayed, "A Comparative Analysis of Symmetric Algorithms in Cloud Computing: A Survey," International Journal of Computer Applications, vol. 182, no. 48, pp. 7–16, Apr. 2019, https://doi.org/10.5120/ijca2019918726.

[22] Chen, Y.; Liu, H.; Wang, B.; Sonompil, B.; Ping, Y.; Zhang, Z. A threshold hybrid encryption method for integrity audit without trusted center. *J. Cloud Comput.* **2021**, *10*, 3.

[23] Sajay, K.R.; Babu, S.S.; Vijayalakshmi, Y. Enhancing the security of cloud data using hybrid encryption algorithm. *J. Ambient Intell. Humaniz. Comput.* **2019**, 1–10.

[24] Latha, K.; Sheela, T. Block based data security and data distribution on multi cloud environment. *J. Ambient Intell. Humaniz. Comput.* **2019**, 1–7.

[25] Cha, J.; Singh, S.K.; Kim, T.W.; Park, J.H. Blockchain-empowered cloud architecture based on secret sharing for smart city. *J. Inf. Secur. Appl.* **2021**, *57*, 102686.

[26] Viswanath, G.; Krishna, P.V. Hybrid encryption framework for securing big data storage in multi-cloud environment. *Evol. Intell.* **2021**, *14*, 691–698.

[27] Xu, Y.; Ding, L.; Cui, J.; Zhong, H.; Yu, J. PP-CSA: A privacy-preserving cloud storage auditing scheme for data sharing. *IEEE Syst. J.* **2020**, *15*, 3730–3739.

[28] Nguyen, G.N.; Le Viet, N.H.; Elhoseny, M.; Shankar, K.; Gupta, B.B.; Abd El-Latif, A.A. "Secure blockchain-enabled Cyber–physical systems in healthcare using deep belief network with ResNet model." *J. Parallel Distrib. Comput.*, 2021, 153, 150–160.

[29] He, J.; Zhang, Z.; Li, M.; Zhu, L.; Hu, J. "Provable data integrity of cloud storage service with enhanced security in the internet of things." *IEEE Access*, 2018, 7, 6226–6239.

[30] Rathore, H.; Mohamed, A.; Guizani, M. "A survey of blockchain-enabled cyber-physical systems." *Sensors*, 2020, 20, 282.