Journal of Integrated
SCIENCE & TECHNOLOGY

Securing Cloud Data: A hybrid encryption approach with RSA and AES for enhanced security and performance

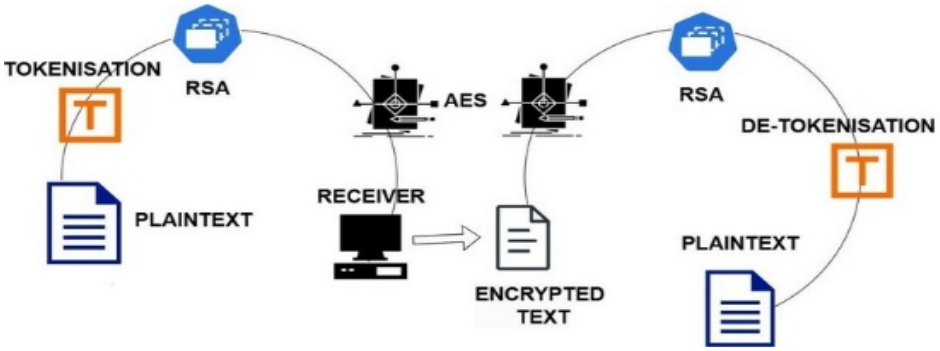
Renuka S. Durge,* Vaishali M. Deshmukh

Computer Science and Engineering, Prof. Ram Meghe Institute of Technology & Research, Badnera-Amravati, Maharashtra, India

Submitted on: 18-Aug-2024, Accepted and Published on: 27-Dec-2024

Article

ABSTRACT In the context of cloud structures, which embrace open spaces for data storage and resource allocation, security has posed the greatest challenge for adopting cloud structures. Even though cloud computing is efficient and has many aspirations, many data security issues still arise because users do not have direct access to their data. A hybrid encryption scheme combining both the RSA and AES (Advanced Encryption Standard) algorithms is proposed to alleviate these issues. The approach consists of converting an appropriate text into bytes and then ciphering the converted bytes using two algorithms: RSA and AES. The text that has undergone this process is called a hybrid combined cipher text. Afterward, the received encrypted data is decrypted using both algorithms to restore the underlying content. This is done also using cloud services, to take advantage of the underlying computing resources and scalability. The performance of the technique is tested by comparing throughput with other key parameters. The obtained results prove the hybrid technique of encryption enhances data security in a cloud setting.



Keywords: Cloud Computing, Data Security, Hybrid Encryption, Byte Encoding, Cloud Platform

INTRODUCTION

Cloud computing has revolutionized the concepts of data organization and distribution of resources by offering more flexible and cheaper options. This strategy allows corporations to utilize huge computing power without the need to buy and maintain facilities. With cloud services, businesses can optimize their operations like never before having a tremendous level of elasticity responsive to demand and workload changes. Nevertheless, this ease of doing business comes with serious security challenges.[1] This is because in addition to being open, in shared cloud environments, data is placed in remote servers located away from the customers and managed by an external cloud vendor which limits[2] the customer's control over their data to a certain extent.

Additionally, the remote system's devotion and lack of control over data contained in the clouds pose certain risks. Users have to be able to convince themselves that the provider has made very good arrangements to keep their data safe.[3] This approach is risky especially to sensitive information since any imperfection in the security structure of the service they are depending on may expose the data to information leaks, hacking, or other such attacks. High-profile instances have shown that even well-established cloud companies are vulnerable to security attacks, emphasizing the significance of strong security standards.

Ensuring the security, integrity, and availability of data in cloud storage is critical yet challenging. Confidentiality ensures that sensitive information is only available to authorized users; integrity assures that data is unchanged throughout storage or transit; and availability ensures that data is accessible.[4,10]

Maintaining the security, consistency and access of data in the cloud Databases is also very important and difficult. Confidentiality means that information is sensitive and is accessed by authorized persons only; Integrity means the storage and transmission of data without any modification and lastly, Availability means data is accessible when required. Encrypting textual information is a

*Renuka S. Durge: Department of Computer Science & Engineering, Prof. Ram Meghe Institute of Technology & Research, Badnera-Amravati. Maharashtra.
Tel: +91- 9975789420 ; Email: renuka434@gmai.com

Cite as: *J. Integr. Sci. Technol., 2025, 13(3), 1060.*
URN:NBN:sciencein.jist.2025.v13.1060
DOI:10.62110/sciencein.jist.2025.v13.1060

standard method of ensuring that sensitive data is read by the appropriate and intended audience only. This simply means covering up all plain text information and presenting authorized personnel with coded version only.[5] Nevertheless, there is a need of more secure methods and algorithms such as the proposed method, to meet unique difficulties such as safe key management, efficient data encryption and decryption, and security against sophisticated cyber-attacks.

The contribution of the paper is given in the following list:

- A large data set is developed to perform the suggested hybrid technique.
- Several prior studies in cryptography and security are compared and analyzed to propose a novel secured approach that can be used for cloud platforms.
- A novel hybrid method with high efficiency is used to improve data security.

Figure 1 illustrates the encrypting and decrypting procedure and how it is utilized effectively using cloud services.

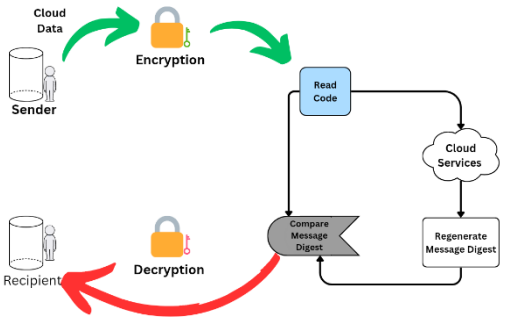


Figure 1: Illustration of the utilization of encryption and decryption in cloud services.

Using RSA and AES for Encryption in Communications

In particular, the RSA algorithm (Rivest Shamir Adleman) is one of the earliest and most widely used asymmetric cryptographic algorithms in common use today. It is based on complex key generation using very large prime numbers and is thus useful in confidentially transmitting encryption keys across unprotected networks[6,7].The AES algorithm (Advanced Encryption Standard) is a symmetric encryption algorithm typically fast in processing even bulk amounts of data. Encryption and decryption employ one key which is shared to both parties, thus most suited for situations where there is a need to protect large amounts of information after exchanging a secure key in a very short period8.

The Role of RSA and AES in Improving Security:

- Double Security System: During this process, RSA encrypts the first step only – the exchange of keys, while AES encrypts the second step, the data itself, very swiftly[9,10]. This ensures efficient key management with fast encryption to the extent that it minimizes the chances of an attack.
- Two Plane Security: Data encrypted with AES is protected with RSA, which in turn protects the AES key[11,12]. Such a security system makes it possible to control access to information while providing high levels of security so that an intruder would not easily penetrate one layer of security and bypass the other.

Literature Survey

This literature survey looks at the progress in cloud encryption and decryption algorithms, focusing on important developments and noting where more research is needed. A review of earlier studies is provided, with the results shown in Table 1.

Table 1: Comparison Table of pre-existing works

Citation	Method	Focus	Advantages	Disadvantages
[1]	Review	Symmetric & Asymmetric Encryption	High security for data at rest and in transit; Efficient for large data sets	Complex key management; Potential performance overhead (asymmetric encryption 10-100x slower than symmetric)
[2]	Comparison	Cloud Storage Encryption	Enhanced data privacy and security; User control over encryption keys	Increased storage costs (10-20% overhead); Potential performance impact for I/O-intensive workloads
[3]	Review	Symmetric & Asymmetric Encryption	Basic understanding of encryption concepts; Suitable for simple use cases	Lacks in-depth analysis of advanced techniques; Limited coverage of real-world security threats
[4]	Analysis	Encryption Algorithms & Machine Learning	Identifies potential vulnerabilities; Leverages AI to improve security analysis	Focuses on theoretical analysis, not practical implementation; Requires significant computational resources and expertise
[5]	Searchable Encryption	Encrypted Cloud Data Search	Enables keyword search on encrypted data; Protects data privacy while maintaining search functionality	High computational overhead (10-100x slower than plaintext search); Complex implementation and limited search capabilities
[6]	Deduplication with Encryption	Cloud Storage Optimization	Reduces storage costs by eliminating duplicate data; Maintains data	Limited to textual data; Increased computational overhead for deduplication and

			confidentiality and integrity	encryption processes
[7]	Multimedia Encryption	Cloud Storage for Multimedia Data	Protects sensitive multimedia content; Supports various multimedia formats (e.g., images, audio, video)	May not be optimized for all multimedia types; Potential performance impact for high-resolution video
[8]	Deduplication with Encryption	Cloud Storage Optimization	Improves storage efficiency and reduces costs; Enhances data security and privacy	Requires specific implementation details and careful configuration; May not be suitable for all types of data
[12]	Secure Search over Encrypted Data	Keyword-based search on encrypted data	Enables secure search on encrypted data; Protects data privacy while allowing for efficient search	High computational overhead (10-100x slower than plaintext search); Limited search capabilities compared to plaintext search
[13]	Hybrid Encryption	Enhanced Security and Efficiency	Combines best of symmetric and asymmetric encryption; Improves performance and security compared to pure asymmetric encryption	Requires careful key management and configuration; Specific performance evaluation details may be limited

Summary of the Table

The table outlines the advantages and disadvantages of each article. This led to a long discussion on how to improve the existing study's inadequacies. This study looks at current resources to identify areas that might be better and suggest novel concepts. The importance and significance of this comparison analysis are increased by recognizing patterns, advantages, disadvantages, and possible solutions for constraints.

DATASET

A combination of two datasets was used: Wikipedia Dumps and Book Corpus. The Wikipedia Dumps dataset consists of a comprehensive collection of articles from Wikipedia, offering a broad and diverse range of topics and writing styles[13,14,15]. This dataset occupies approximately 60 GB of memory, providing ample data for diverse contextual understanding Table 2 displays an example of a Wikipedia Dumps entry. In contrast, the Book Corpus dataset consists of text from a wide collection of books across numerous genres. This diversity makes it particularly useful for encryption tasks. An example of the Book Corpus dataset is shown in Table 3.

Table 2. Example of the Book-Corpus Dataset

Title	Content
Quantum Computing: A New Era of Computation	Quantum computing represents a revolutionary advancement in computational power. By harnessing the principles of quantum mechanics, these systems can process vast amounts of information simultaneously, enabling solutions to complex problems that are intractable for classical computers. This technology holds immense potential to transform various fields, including drug discovery, materials science, artificial intelligence, and cryptography.

Table 3. Example of Wikipedia Dumps Dataset

Title	Content
Twilight's Embrace	As the sun descended, casting elongated shadows across the cobblestone street, Elara hastened her pace. The air was heavy with the promise of rain, a distant rumble of thunder echoing through the gathering dusk.

METHODOLOGY

The proposed methodology for enhancing data security in cloud environments involves a dual-layer encryption technique combined with byte-level tokenization[16]. Initially, the input text is processed using the Byte- Level Encoding of Byte Pairs (BPE) tokenizer. This tokenizer transforms the raw text into a sequence of byte- level tokens by iteratively merging the most frequent byte pairs found in the text[17]. This process not only reduces the vocabulary size but also efficiently handles out-of-vocabulary words, making the text representation more compact and manageable.

$$Token\_\{i+1\} = Merge(Token\_i, BytePair) \quad (1)$$

Following tokenization, the data undergoes encryption using the RSA algorithm, a well-established public-key cryptosystem[18]. RSA encryption begins with key generation, where two large prime numbers p and q are selected to create public and private keys. The modulus n is calculated as:

$$n = p \times q \quad (2)$$

The public key (e, n) is generated, where e is the public exponent[19]. The private key (d, n) is calculated using the private exponent d which is derived from

$$e \times d \equiv 1\ (mod\ (n)) \quad (3)$$

where φ(n) = (p-1) × (q-1) is Euler's totient function[20]. The plaintext, represented as a sequence of tokens m, is encrypted using the public key to produce ciphertext c:

$$c=m\text{^}(modn) \quad (4)$$

This ciphertext can only be decrypted with the corresponding private key, ensuring that the data remains secure from unauthorized access. To further enhance security, the RSA-encrypted data is subjected to an additional layer of encryption using the Advanced Encryption Standard (AES)[21,22]. AES is a symmetric-key encryption algorithm that operates on fixed-size blocks of data

and employs multiple rounds of transformations, including substitution, permutation, and mixing. The same key k is used for both encryption and decryption, which adds another layer of protection to the data. During the decryption process, the sequence is reversed to retrieve the original data[23].

$$AES\_Encrypt\ (c, k)\ =\ Ciph\ ertext \quad (5)$$

The AES-encrypted data is first decrypted using the AES key to recover the RSA-encrypted text:

$$AES\_Decrypt\ (Ciph\ ertext, k) \quad (6)$$

Next, RSA decryption is performed using the private key to obtain the tokenized text:

$$m = c\text{^}d\ (mod\ n) \quad (7)$$

Finally, the Byte-Level BPE tokenizer is employed to detokenize the data and restore the original text, completing the decryption process.

$$Original\_Text{=}Detokenize\ (Token\_\{i + 1\}) \quad (8)$$

This dual-layer encryption approach, combined with byte-level tokenization, provides robust protection for sensitive data, enhancing its security against potential breaches and unauthorized access[24,25]. The proposed methodology is represented in below Figure 2

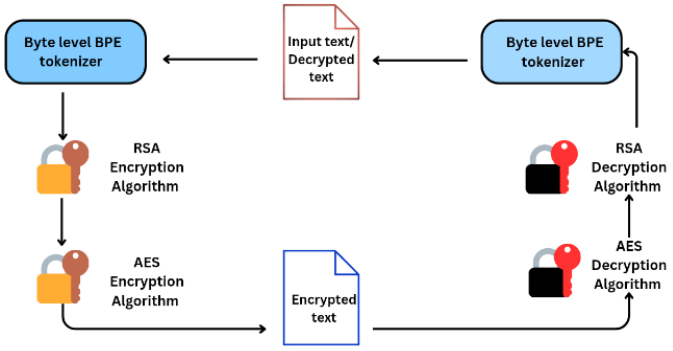


Figure 2: The Architecture of the proposed methodology

System Configuration:

The system for testing the hybrid RSA-AES encryption method is built for high performance. It includes an Intel Core i9-11900K processor (8 cores, up to 5.30 GHz) and 32 GB DDR4 RAM for smooth handling of encryption tasks. Data storage is managed by a 1 TB NVMe SSD for quick read/write speeds. An NVIDIA GeForce RTX 3080 GPU supports additional processing needs and dual-boot options for Windows 10 Pro and Ubuntu 20.04 LTS offer flexibility with encryption tools. 1 Gbps Ethernet connectivity enables fast network data transfers, ideal for cloud-based encryption.[26]

RESULTS

The model's outcome highlights the strength of layered encryption in delivering strong security. The fixed-length output produced by RSA encryption17,18, coupled with the additional Fernet encryption layer, guarantees the protection of the encrypted data and the integrity of the encryption procedure. Security Features and Resistance to Attacks of Encryption Algorithms is shown in the below table 4, A Graphical representation of Throughput vs Algorithm is shown in the below Fig 3. Table 5 compares how well different encryption methods handle large data in cloud systems.
For example: "Today is Monday".
By utilizing a byte-level BPE tokenizer, it is tokenized.

Input Text: "Today is Monday"
Using a byte-level BPE tokenizer :

Tokenized Output: [123, 5678, 432, 3456]

Through tokenization, the text is changed into a series of token IDs, which are the text's numerical representations. The tokenized output is then encrypted using RSA after that. Regardless of the input size, RSA encryption with a 2048-bit key generates a 256-byte cyphertext. Below is the result of the RSA encryption.

RSA Encrypted Data: gAAAAABlni1tGHicp3ODvH1X-rwdf-sf8vbvPZiV4Xn2p5y6q1T8u8fdh5yG73t8TGmZGhD5qXEvbC8z N3X94r8RYXtbW5d6C4n-zFyFtmFeN5KxLhES0soFwvOCXp_tskqsmRa7a2TVkA6OYZv U_t5PSxWgXCR Q4sh3zJ7tNDRbwqaSZDg2s8J9QzNQyI9HqwPcgTZ5SOp8B93 X0XyO8HvFPZp3n3MJ8RV8gO8OFA8I7jFZ qELh8MQaeS2oCmHK2ULJnvDlGF_wTYF5f3kOk5Hf5SwU1B yq4iyHaeC2s3t5S4Ak0PzyOU4R9tX_J6HpG 4dtHbV5ZV7q6M0I6G0Iu2Z7i3Hkzmr7d1dEzhQ2Y5xjs

In the next step, the encrypted cipher text from RSA is again encrypted using the AES. AES is used in the cipher block chaining (CBC) paradigm with a 128-bit block size19 to further encrypt the RSA-encrypted data. The Fernet ciphertext has a length of 440 bytes. Because Fernet encryption adds a version byte, timestamp, initialization vector, and HMAC for integrity checks, the length is more than the RSA ciphertext. Additionally, the Fernet employs padding, which expands the size.

Encrypted AES Cipher Text:

gAAAAABlni1x2PYWGVK74pzTxnbEeoHEUmpcxT8ilHgX OD8X0XyFAk8JhPZWmF9V63rEYf2sPqZLUt HZr5M2AjgHgkXdnzHYK1H2fuvLqbsRzD_mHX3QDQzM0Zs ED2k26G3Z2A9w9lbQ0Qx5udSkEGlXLaiZ6 smjpB4VfHlqpzicTXH4trp7tJpW7LsLKHZ4HIFkA1TnmS8GQJ rcdHeKFxJ4mZphRl6lH83ff7RlgsGVfoYFq9 hgyBCkO_Yk_eLr1Fs33efXGZSwD0K1clW8Qk6l5Ig2UVKvH M4r8WZJeHqUqHj7m3Lw9X7bmttRWr3NK OxA09kvHUBtN5l3W4ts7q3dF3ZqA5_Ja1HqGQxQ8ONqjQv5T tQgwFxL0. Now the cipher text is ready. Now when this has to be back to its form by users, Decryption works20. To retrieve the

cipher text of RSA, we must first decrypt the cipher text received via AES. Below is the decrypted text of the AES cipher.

Decrypted AES Ciphertext: \x83\xfd\xbd\xaf\xa2\x04\xc4\x1e\xfa\x96\x7f\xcc\xec\x03\x91\xd5\x12\xcf\x82T\xa7\xea\xfb\x95H\x1f\x02O\xdb\x8e9\x05\xbe\xd8D\xf3\xec\xd5o\xb8X\x16\xbf\xbd\x94\xa6\xae\x90\xd0\xc2B\xbf7\xf5\x98\x7c\xdc\xf6\x08J\xd1\x1c\x1c\xb4F\xd8\xa6\x12\xde\x1c\xd3a\xea\x0f\x1e\x8b\xf5\xbe\x04Y\nG\x0e\x8a\xd4\x93\x07\xbc\x87\x08Q\xd3\xc0\x85\x8a\xb8\x84\xbdF\xae\xb0O\xecU\x05f\xd5\xd7E\xde\x0b\xbeT\xff\x94l5\xd5\xef\xd5\x0f\x8c2\x03\xf7\xcb\xac1\x14\xfb\xdd\xe2\x8c\x0b3\x87\xea\x8f\x0b\xd5\x13E\x05\xfe\x14\x83

Decrypting the RSA ciphertext to get the original tokenized Tokenized Output (After RSA Decryption): [123, 5678, 432, 3456] Reconstructing the Original Text Finally, converting the token IDs back into the original text:

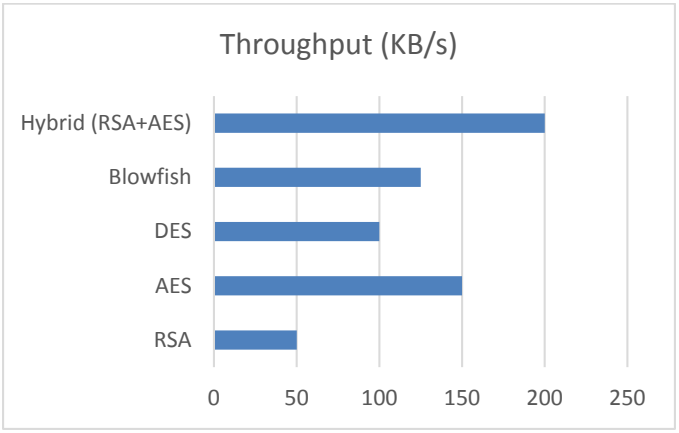
Reconstructed Text: "Today is Monday".

Table 4: Security Characteristics and Attack Resistance of Various Algorithms

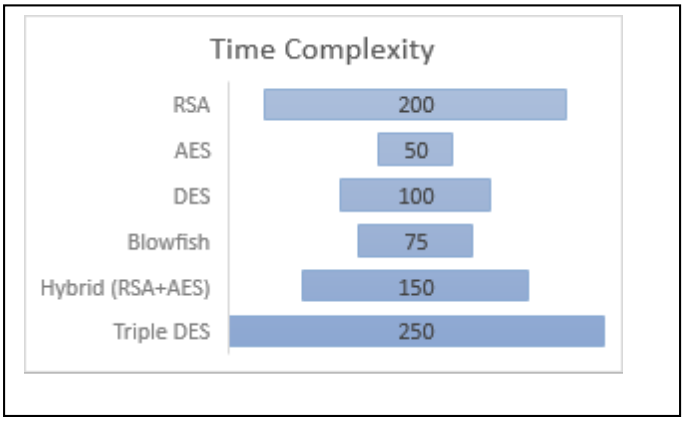
Algorithm	Key Length (bits)	Security Level	Resistance to Attacks
RSA	2048	High	Moderate resistance to quantum attacks
AES	256	Very High	Strong resistance to most attacks
DES	56	Low	Weak and easily broken
Blowfish	448	High	Strong resistance to most attacks
HybridRSA-AES	2048 (RSA) + 256 (AES)	Very High	Strong resistance to both classical and quantum attacks due to combined strengths

Table 5: Security Features and Scalability

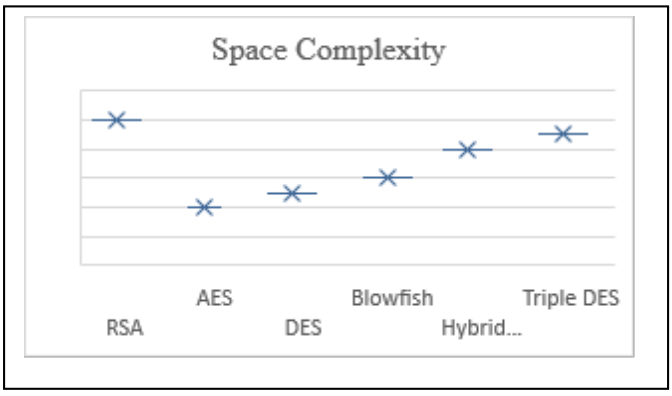
Algo	Key Management Complexity	Data Integrity Check Method	Brute Force Resistance	SideChannel Resistance	Chosen Ciphertext Resistance	Small File Performance (ms)	Large File Performance (ms)
RSA	High	Hashing	Medium	Low	Medium	250	1000
AES	Low	HMAC	High	High	High	50	120
DES	Low	None	Low	Low	Low	90	300
Proposed Model	**Medium**	**HMAC + Hashing**	**Very High**	**High**	**Very High**	**150**	**500**



3(a)



3(b)



3c)

Figure 3: Comparative Analysis of various a) algorithms Throughput b)Time Complexity vs Algorithm c) Space Complexity vs Algorithm

Types of attacks prevented by the proposed hybrid approach

This hybrid RSA-AES approach is developed to provide good security against all the above types of attacks:

- Brute-force attacks. Due to the sizes of RSA keys in bits (2048–4096) and AES keys in bits (128–256), it is almost impossible to crack the keys by trying every possible combination[23].
- Side-Channel Attacks: The dual-layered encryption minimizes the risks from side-channel

attacks, since attackers would have to bypass both RSA and AES layers.

- Chosen Ciphertext Attacks (CCA): RSA encryption, when used as a first layer, visibility to only encrypted data exists, which reduces the impact of CCA.
- Replay and Man-in-the-Middle Attacks: With AES combined with RSA for key exchange, no data can be read nor replayed easily

CONCLUSION

In the context of cloud computing, security problems still arise as there is very little physical control of the data. This paper addresses the issue by suggesting a hybrid encryption technique, using both RSA and AES encryption methods[22]. The method involves encoding, dual-layer encryption using RSA and AES, and removing the encryption to get back the original data[24], effectively making use of the cloud resources to boost the security performance. Assessment based on time and space complexity, and throughput of the technique's impact on data security indicates the technique places an answer on the problem of data security in clouds[25]

FUTURE SCOPE

There are numerous possible future researches on the hybrid RSA-AES encryption technique. For example, it is possible to adapt this approach for real-time data security applications, which would require video encryption and live data streaming. Here, what is necessary is that good security has to be ensured while being under latency constraints. One more promising prospect is the quantum-resistant cryptographic algorithms' integration into ensuring future security against threats on quantum computing to prevent sensitive information compromise[18,26]. Moreover, integrating AI-based anomaly detection would enhance the resilience of the system in the sense that it can easily identify and respond to unauthorized access or abnormal activity attempts. Generalizing this technique further into IoT and edge computing environments will make it optimize toward resource-constrained devices through low power consumption and bandwidth efficiency. Improvements such as these put the hybrid RSA-AES encryption technique in a strong yet adaptive position in the ever-changing tides of data security

CONFLICT OF INTEREST STATEMENT

The authors state that there is no conflict of interest in the paper.

REFERENCES AND NOTES

1. K.H. Al-Khafaji, H.A. Sahib. Designing a Digital System for Enhancing,Coloring, Encryption and Decryption of X-ray Medical Image. In *2024 15th International Conference on Information and Communication Systems, ICICS 2024*; Irbid, Jordan, **2024**; pp 1–6,.
2. S. Devi, H.S. Vinay Kumar. Simple Encryption and Decryption of Password for Cyber Security Application. In *2024 4th International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies, ICAECT 2024*; Bhilai, India, **2024**; pp 1–5,.
3. X. Zhang, J. Wang, N. Li, Y. Xu. Design and implementation of automatic encryption and decryption system in configuration center based on etcd. In *2024 4th International Symposium on Computer Technology and Information Science, ISCTIS 2024*; Xi'an, China, **2024**; pp 321–324.
4. M.D. Bharathi, B. Latha. A deep study of analysis for encryption and decryption algorithm in cloud data with machine learning techniques. In *2024 International Conference on Communication, Computing and Internet of Things, IC3IoT 2024 - Proceedings*; IEEE, **2024**.
5. S. Yin, H. Li, L. Teng, A.A. Laghari, V.V. Estrela. Attribute-based multiparty searchable encryption model for privacy protection of text data. *Multimed. Tools Appl.* **2024**, 83 (15), 45881–45902.
6. K. Ghassabi, P. Pahlevani. DEDUCT: A Secure Deduplication of Textual Data in Cloud Environments. *IEEE Access* **2024**, 12, 70743–70758.
7. P. Saini, K. Kumar. S-method: secure multimedia encryption technique in cloud environment. *Multimed. Tools Appl.* **2024**, 83 (3), 8295–8309.
8. R. Ganesamoorthy, G. Pushpa, B. Senthilkumar, et al. A Novel Design of an Image Encryption and Decryption Scheme Using Enhanced Cybersecurity Principles. In *1st International Conference on Emerging Research in Computational Science, ICERCS 2023 - Proceedings*; India, **2023**; pp 1–6,.
9. S.P.P.M.B. Kumaraswamy S, Ananth Prabhu Gurpur, Akashraj Raga. Enhancing Data Privacy Protection in Cloud Computing Through Ciphertext-Policy Attribute-Based Encryption. *J. Electr. Syst.* **2024**, 20 (3s), 1113–1124.
10. G. Lin, W. Hua, Y. Zhang. EmojiCrypt: Prompt Encryption for Secure Communication with Large Language Models. **2024**.
11. K. Selvakumar, S. Lokesh. A cryptographic method to have a secure communication of health care digital data into the cloud. *Automatika* **2024**, 65 (1), 373–386.
12. N. Singh, J. Kumar, A.K. Singh, A. Mohan. Privacy-preserving multi-keyword hybrid search over encrypted data in cloud. *J. Ambient Intell. Humaniz. Comput.* **2024**, 15 (1), 261–274.
13. A.N. Bhat, R. Kumar. Efficient Hybrid Encryption Algorithm for Securing Data in Cloud Environment. April 18, 2024.
14. S. Li, X. Deng, Y. Zou. RR-Raft: A Raft Consensus Algorithm Based on Reputation Regression Model and RSA Signature. In *Proceedings - 2024 2nd International Conference on Mobile Internet, Cloud Computing and Information Security, MICCIS 2024*; Changsha City, China, **2024**; pp 92–96.
15. Z. Wang, D. Han, J. Hou. Design of Dual Code Traceability System for Agricultural Products Based on RSA Algorithm. In *Proceedings - 2024 Asia-Pacific Conference on Software Engineering, Social Network Analysis and Intelligent Computing, SSAIC 2024*; New Delhi, India, **2024**; pp 83–88.
16. J. Hu, F. Yan, Z. Wu. BGRAFT: Grouped Anti-Byzantine RAFT Consensus Algorithm Based on RSA Encryption Algorithm. In *Proceedings - 2024 International Conference on Artificial Intelligence and Digital Technology, ICAIDT 2024*; Shenzhen, China, **2024**; pp 279–283.
17. N. Syanti, M.A. Budiman, Sawaluddin. Real Running Time Analysis of Multi Prime RSA Algorithm and XRSA in Securing Digital Messages. In *Proceeding - 2024 International Conference on Information Technology Research and Innovation, ICITRI 2024*; Jakarta, Indonesia, **2024**; pp 287–292.
18. L. Yaping, Z. Zhang, P. Xie, et al. Joint Optimization of Working and Protection Paths for RSA in Mixed-Grid Optical Networks. In *2024 22nd International Conference on Optical Communications and Networks, ICOCN 2024*; Harbin, China, **2024**; pp 1–3,.
19. V. Valsan, K.K. Keerthan, N.S. Devnath, A. Ajithkumar, A. Sasikumar. Securing Sustainable Energy Trading: An RSA-Encrypted IoT Solution for Smart Meter Data Transmission. In *Proceedings - 2024 International Conference on Computational Intelligence and Computing Applications, ICCICA 2024*; Samalkha, India, **2024**; pp 187–192.
20. M. Bhavitha, K. Rakshitha, S.M. Rajagopal. Performance Evaluation of AES, DES, RSA, and Paillier Homomorphic for Image Security. In *2024 IEEE 9th International Conference for Convergence in Technology, I2CT 2024*; Pune, India, **2024**; pp 1–5.
21. V. Saicheur, K. Piromsopa. An implementation of AES-128 and AES-512 on Apple mobile processor. In *ECTI-CON 2017 - 2017 14th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*; Phuket, Thailand, **2017**; pp 389–392.

22. N. Cherrid, R. Saidi, T. Bentahar, H. Mayache. Study of the Sensitivity of an InSAR Interferogram Encrypted by the AES-128 Algorithm. In *18th IEEE International Multi-Conference on Systems, Signals and Devices, SSD 2021*; Tunisia, **2021**; pp 457–462.
23. H.S. Deshpande, K.J. Karande, A.O. Mulani. Efficient implementation of AES algorithm on FPGA. In *International Conference on Communication and Signal Processing, ICCSP 2014 - Proceedings*; Melmaruvathur, India, **2014**; pp 1895–1899.
24. S. Liu, Y. Li, Z. Jin. Research on Enhanced AES Algorithm Based on Key Operations. In *Proceedings of 2023 IEEE 5th International Conference on Civil Aviation Safety and Information Technology, ICCASIT 2023*; Dali, China, **2023**; pp 318–322.
25. K. Gurugubelli, S. Mohamed, K.S. Rajesh Krishna. Comparative Study of Tokenization Algorithms for End-To-End Open Vocabulary Keyword Detection. In *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*; Korea, Republic of, **2024**; pp 12431–12435.
26. M. Hossain, R. Khan, S. Al Noor, R. Hasan. Jugo: A Generic Architecture for Composite Cloud as a Service. In *2016 IEEE 9th International Conference on Cloud Computing (CLOUD*; San Francisco, CA, USA, **2017**; pp 806–809.

BIOGRAPHIES OF AUTHORS

Renuka Shone Durge holds Phd degree in Cmputer Science and Engineering and done B.E.,M.E from Sant Gadge Baba University, Amaravati. Maharashtra India. She is currently a Lecturer in Government College of Engineering Amravati. India. Areas of specialization of the author is in the domain Cloud Computing and doing research work on cloud security system.

Vaishali H. Deshmukh holds a Phd degree in Computer Science and Engineering and done B.E, M.E from Sant Gadge Baba University, Amaravati. Maharashtra India, she is currently a Professor in Department of Computer Science & Engineering Prof. Ram Meghe Institute of Technology and Research, Badnera-Amravati. India. Areas of specialization of the author is in the domain Algorithmics, System Software and have published more than 64 international papers.