P-ISSN 1991-8941
E-ISSN 2706-6703
Vol. 19, No. 2 (2025)

Journal of University of Anbar for Pure Science
(JUAPS)

journal homepage: juaps.uoanbar.edu.iq

Open Access

Original Paper

A hybrid cryptosystem for cloud security: combining Okamoto-Uchiyama and Advanced Encryption Standard for optimized encryption performance

Azhar Malik [1*]

[1]Computer Engineering Department, University of Technology, Baghdad, Iraq.

ARTICLE INFO

Received: 15/03/2025
Accepted: 30/04/2025
Available online: 08/11/2025
December Issue
10.37652/juaps.2025.158225.1364

CITE @ JUAPS

Corresponding author
Azhar Malik
azhar.m.alnaseri@uotechnology.edu.iq

ABSTRACT

The central challenge in cloud computing is delivering strong data protection while maintaining high system performance. This paper addresses the problem by developing a hybrid cryptosystem that integrates the strengths of Okamoto-Uchiyama (OU) and Advanced Encryption Standard (AES). For key transfer, the model employs secure OU public-key encryption to prevent key compromise in transit, and AES for fast symmetric encryption of large data bursts when required. As a result, AES handles data encryption operations while OU was used solely for key exchange, avoiding the usual overhead associated with asymmetric encryption. The hybrid system was deployed in the cloud and compared with asymmetric models such as RSA. Test results showed that the proposed system outperforms existing approaches by reducing encryption and decryption times by nearly 90% for large-scale data without compromising security. It also provides extended resistance to common attacks, including brute-force and man-in-the-middle (MITM) attacks, supporting its practical applicability in cloud environments. The hybrid cryptosystem offers an optimal balance of performance and security, making it suitable for current cloud computing applications such as SaaS, PaaS, and IaaS.

Keywords: *Advanced Encryption Standard, Cryptography, Okamoto-Uchiyama, Private key, Public key*

1 INTRODUCTION

Cloud computing has emerged as a crucial business tool in today's highly dynamic technological landscape for administration across sectors and on-demand resource management. However, growing reliance on cloud-based services raises concerns about data security, specifically the confidentiality, integrity, and availability of data. Some encryption approaches, while conventional for protecting data, struggle to deliver strong security with optimal performance in cloud settings [1]. This makes it necessary to develop improved cryptographic systems that secure data without compromising performance. The proposed hybrid cryptosystem addresses this need by combining two robust techniques: the Okamoto–Uchiyama (OU) public-key scheme and the Advanced Encryption Standard (AES). This approach leverages asymmetric and symmetric encryption to provide a model that delivers optimal encryption performance without compromising security [2]. In particular, the OU cryptosystem is included in secure key exchange, which is an option that fulfills the need to preserve confidentiality when transmitting keys. AES on the other hand, performs the major task of encryption, thus making it easy and fast to encrypt and decrypt big data. In this regard, the proposed hybrid model reduces the overhead inherent in many asymmetric encryption methods, such as RSA, by shifting complex calculations to AES [3]. This research is motivated by the absence of an encryption system that fully meets cloud computing security requirements while overcoming the performance drawbacks typical of such systems. Common cryptographic techniques, including RSA, slow down notably when large data sets are processed [4]. It is expected that the proposed system, using OU for secure key management and AES for fast data encryption, will improve cloud security models without compromising response time or capacity. The first contribution of this paper is a dual-layer cryptographic security solution with enhanced encryption efficiency.

The proposed hybrid system shows improvements in count and time compared with a traditional asymmetric cryptography system, particularly for large-scale data in cloud databases. Furthermore, the system's effectiveness against basic attempts such as brute-force and man-in-the-middle attacks supports the applicability of the concept for protecting data in healthcare, finance, and government. Accordingly, this study presents a systematic approach to addressing data-security issues in the cloud while integrating security requirements with the functionality of large-scale data infrastructures. The hybrid cryptosystem is an efficient, scalable, and secure architecture prepared to support additional cloud service models.

2 LITERATURE REVIEW

Because of the rapid adoption of cloud computing in businesses, user data must be shielded from external risks, with provisions for greater storage capacity and faster access. Traditional techniques such as RSA face disadvantages as data volumes grow, often becoming very large in many applications. This paper proposes a new bi-level cryptographic strategy that combines the Okamoto–Uchiyama (OU) public-key encryption technique and the Advanced Encryption Standard (AES). Secure key exchange is performed by OU, ensuring confidentiality in key distribution, while AES handles bulk data encryption to maximize speed. This dual paradigm offloads compute intensive tasks to AES and, overall, provides better performance while retaining security. The proposed cryptosystem is deployed in a cloud environment, where it exhibits lower encryption time than conventional approaches, making it relevant to service-based environments such as SaaS, PaaS, and IaaS. The mixed method also enhances system flexibility and resistance to modern decryption techniques, making it suitable for sectors such as health, finance, and government. Additional research is conducted on the effective application and optimization of the Gronsfeld cipher key via the Okamoto–Uchiyama public-key cryptosystem to improve data security [1]. The authors also demonstrate that OU can improve key generation and encryption speed, indicating its suitability for secure data transmission systems. This study views OU as a means of enhancing encryption algorithms through improved key handling. The protection of medical data in the cloud is addressed by a hybrid approach that combines Okamoto–Uchiyama homomorphic encryption with Euclidean distance [2], Figure 1. This paper demonstrates how combining these techniques enhances security and data-handling efficiency in applications involving sensitive and confidential healthcare records for cloud-based medical use. A secure cloud methodology is proposed using the Okamoto–Uchiyama cryptosystem to demonstrate the security of cloud-stored data [3]. The paper illustrates how OU can mitigate cloud-security risks and strengthen data protection against cyber threats in DC settings. It also elaborates a practical hybrid cryptographic model that employs multiple encryption techniques to safeguard data stored on cloud servers [4], as shown in Figure 2. The authors highlight that employing multiple cryptographic algorithms improves cloud security while enabling fast encryption, which is particularly useful for large-scale cloud services.

This work examines novel cryptographic approaches to cloud security, surveying methodologies and designs aimed at enhancing the effectiveness of cloud encryption. Using both symmetric and asymmetric encryption, the authors explain how integrating the two can increase security and efficiency in cloud computing applications [5]. Paper [6] developed a hybrid cryptosystem that incorporates both Paillier and RSA to improve security for big data. According to the authors, the hybrid system elevates security for large datasets while addressing computational barriers often associated with encryption in big-data and cloud environments. The overall improvement of cloud data safety through integrating RSA and AES encryption is also explored [7]. The proposed model offers faster encryption and stronger security than plain RSA and is therefore well suited to cloud computing, where large volumes of data require efficient encryption. The utilization of the NTRUEncrypt method for improving information security in big-data systems should also be discussed and analyzed. This cryptographic approach is increasingly used for securing large data stores in the cloud, supporting the effectiveness of hybrid protection in big-data contexts [8]. It also offers an efficient method within the Hadoop ecosystem to secure information delivered in that environment.

The authors outline a mixed-encryption methodology to address security vulnerabilities in big-data structures while emphasizing the need for cryptographic optimizations to enhance platform performance [9]. They propose improving information security in Hadoop using a hybrid encryption approach [10]. The method enhances the security and efficiency of big-data systems, especially in cloud settings, through multiple encryption techniques.

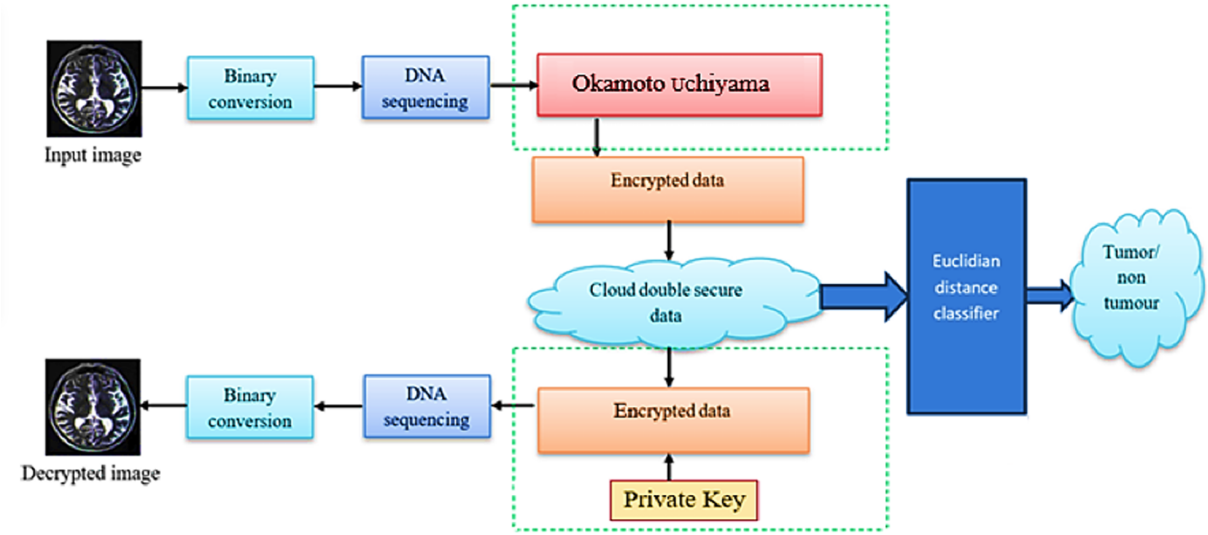

Fig. 1 Double secure cloud medical data [2]

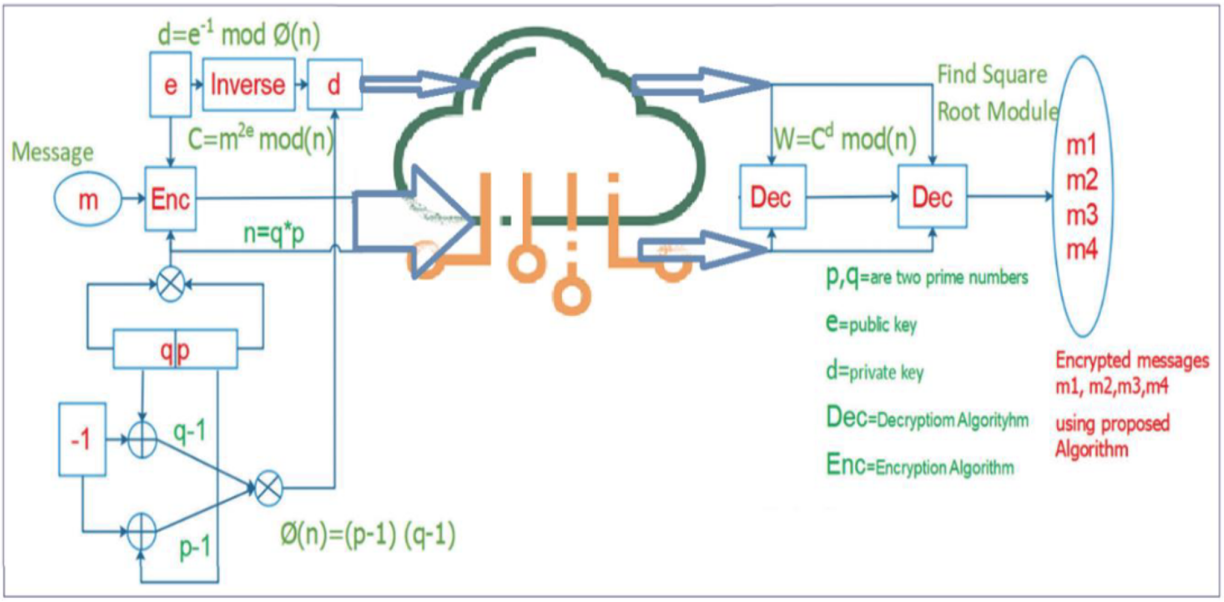

Fig. 2 Robust Hybrid Cryptographic Approach in Cloud [4]

The study presents a compact and relatively robust encryption methodology to secure cloud-stored data, balancing the trade-off between cryptographic speed and security for generalized cloud applications [11]. The authors also propose an RSA–NTRU-based, two-layered cryptographic model for securing cloud data [12]. The hybrid model accelerates key-exchange processes, making it suitable for large-scale cloud environments that require data encryption. Paper [13] introduces a new approach to mining and aggregating IoT sensor data using a hybrid cryptosystem. The adopted hybrid model improves the security of IoT applications in the cloud, as well as the protection of data during storage and transfer. Other work provides a brief review of design vulnerabilities and protections for cybersecurity wallets and proposes cryptographic approaches for optimal wallet safeguards. The findings are relevant to cloud environments where higher levels of data security are required [14].

In particular, an advanced hybrid encryption scheme combined with AuthPrivacyChain has been proposed to optimize cloud versatility and security [15]. This system integrates blockchain with hybrid cryptography to enable safe and scalable cloud applications. Paper [16] presents an overview of hybrid cryptographic mechanisms in cloud computing with an emphasis on security and performance enhancements, demonstrating improved encryption optimization for cloud storage and processing. Paper [17] discusses hybrid encryption schemes as a security model for web applications in cloud computing, incorporating security controls to protect cloud-hosted web apps against cyber threats without compromising manageability or performance. Paper [18] reviews the hybrid encryption approach for improving cloud-data security, focusing on confidentiality and reliability using both symmetric and asymmetric algorithms. A new concept of a phylo-cryptographic model is also presented to enforce security measures in the cloud-computing environment. That is why the model contributes to encrypting and safeguarding large datasets in distributed cloud settings to enhance computing-environment security [19]. Paper [20] introduces mixed cryptographic methods for secure data management in the cloud, emphasizing more effective key exchange and encryption. The authors show how the system can recover from attacks and argue it is a good candidate for cloud services. A general hybrid encryption scheme for clouds is proposed, with improved methods designed to enhance both speed and security. Thus, the proposed hybrid system offers a realistic chance to protect cloud data at large scale [21]. New cryptographic approaches are introduced for enhancing cloud security. The hybrid methods proposed by the authors increase data confidentiality and improve system performance, making them suitable for service oriented cloud systems [22]. Paper [23] proposes a new hybrid encryption algorithm using Twofish to improve security in cloud settings, aiming to enhance both experimental efficiency and the safety of cloud-stored data. Paper [24] develops improved file storage architecture in the cloud using hybrid cryptographic techniques; the model enhances security and performance by protecting and securely transmitting large datasets. Paper [25] discusses protecting big-data storage in cloud systems with hybrid cryptosystems, which augment data security and support efficient management and storage. Paper [26] designs a lightweight hybrid cipher to improve cloud-data security in parallel computing systems, minimizing the trade-off between key-encryption speed and security while enabling fast protection in distributed clouds. Paper [27] describes a new hybrid method for key and data exchange in a cloud environment; integrating the two systems improves security and performance, making it suitable for secure communication. Paper [28] presents a novel approach to securing and compressing data streams by combining methods within cloud infrastructure, enhancing transmission security while reducing storage requirements for large-scale applications.

3 METHODOLOGY

A hybrid cryptosystem was designed, implemented, and systematically evaluated using OU public-key encryption and AES symmetric encryption. This methodology provides a subset of essential security measures while delivering strong performance under cloud computing conditions.

3.1 System design and architecture

By combining asymmetric and symmetric cipher functions, the hybrid model capitalizes on the strengths of both paradigms:

- **Asymmetric Encryption (Okamoto–Uchiyama):** OU was selected for secure key exchange because it provides reliable public-key encryption. Keys can be shared in untrusted environments, which is crucial for cloud systems.
- **Symmetric Encryption (Advanced Encryption Standard):** AES was employed for bulk data encryption and decryption. The symmetric algorithm was chosen for fast, effective processing in big-data and cloud settings.

In operation, OU performs the secure exchange of AES keys, while AES executes the actual encryption of large data volumes. This division minimizes computational cost for large-scale workloads and maintains a high level of security during key exchange.

3.2 Key generation and distribution

The key-management process applies two layers of encryption to ensure secure exchange and rapid data protection. **OU key generation:** Two large primes p and q were selected to generate public and private key pairs. The public key was shared within the cloud, and the private key remained securely held by the owner. The OU public key encrypted the AES key prior to transmission.

AES symmetric key generation: A session AES key was created for the specific encryption task. Known only to sender and recipient, it was used to encrypt cloud data. The AES key was then encrypted with the recipient's OU public key and transmitted. Upon receipt, the recipient used the OU private key to decrypt the AES key and then applied that key for bulk encryption/decryption of the data.

3.3 Encryption process

AES encryption of data: Data to be stored or transmitted were first encrypted with AES. AES offers high throughput and is well suited to large datasets in cloud environments. The AES key used for data encryption was protected with the recipient's OU public key and sent securely. After decryption on the recipient side with the OU private key, the same AES key enables efficient bulk encryption and decryption of the payload.

3.4 Decryption process

The recipient was first decrypted the AES key using the OU private key, ensuring uncompromised key exchange. The recovered AES key was then used to decrypt the ciphertext. Because AES is performance-optimized, this step is fast and supports timely access to the decrypted data.

3.5 Implementation in cloud environment

The hybrid cryptosystem was deployed in a cloud environment using a distributed architecture on virtualized servers to handle encryption and decryption efficiently. **Data flow:** Data were encrypted with AES before cloud storage, and the AES key was shared via OU encryption, preserving confidentiality across distributed storage nodes. **Cloud service models:** The system is exercised across SaaS, PaaS, and IaaS to demonstrate adaptability to different architectures and use cases. **Security analysis:** Large key sizes were employed: AES supports 128-, 192-, or 256-bit keys, and OU relies on large primes, providing high-level security and resistance to brute-force attacks. **Man-in-the-middle (MITM) attacks:** OU protects key exchange so that only the intended recipient can decrypt the AES key with the corresponding OU private key. The dual-layer model supports data integrity by preventing undetected modification under strong encryption mechanisms.

4 RESULTS AND DISCUSSION

The following mathematical model demonstrates the integration of the hybrid cryptosystem: Okamoto–Uchiyama (OU) public-key encryption for secure key exchange and the Advanced Encryption Standard (AES) for rapid data encryption.

4.1 Okamoto-uchiyama (ou) public key encryption

The Okamoto-Uchiyama cryptosystem is an asymmetric encryption method. Below are the mathematical operations involved in its key generation, encryption, and decryption processes.

Key Generation: Prime Numbers: Two large prime numbers, p and q, are chosen such that:

$$n = p^2 q \tag{1}$$

Public Key: The public key $(n, g)(n, g)(n, g)$ is defined as: $n = p^2 q$, and $g = 1 + p$. and the

Private Key: The private key p is kept secret.

Encryption (OU): To encrypt a message m, where $m$is the AES key in this hybrid system:

Select a random number $r \in Z_n^*$ (random integer less than n).

1. Compute the ciphertext c as: $c = g^m r^n \bmod n$

Decryption (OU): To decrypt the ciphertext c and retrieve the message m (AES key), the following steps are performed using the private key p:

1. Compute $c^{p-1} \bmod p^2 \ : \ L(x) = \frac{x-1}{P}$ where $x = c^{p-1} \bmod p^2$.

2. Recover the message m (AES key) as:

$$m = \frac{L\left(c^{p-1} \bmod p^2\right)}{L\left(g^{p-1} \bmod p^2\right)}$$

4.2 Advanced encryption standard (aes)

AES is a symmetric key encryption algorithm used to encrypt large datasets in a hybrid system. The mathematical model for AES encryption and decryption is summarized below.

Key Expansion: AES expands the initial symmetric key into a series of round keys. The key expansion algorithm operates as follows:

- The initial AES key K (128-bit, 192-bit, or 256-bit) is used to generate multiple round keys.
- The key schedule involves a series of bitwise operations, substitutions, and rotations to generate round keys for each encryption round.

Encryption (AES): AES encryption of data is performed using a series of transformation rounds:

- AddRoundKey: The plaintext data P is XOR with the first-round key $K0 : P' = P \oplus K0$
- SubBytes: The bytes of P' are substituted using an S-box (non-linear substitution).
- ShiftRows: The rows of the resulting matrix are shifted.
- MixColumns: A linear transformation is applied to each column of the matrix.
- AddRoundKey: The output of the previous round is XORed with the next round key Ki.

These steps are repeated for a certain number of rounds (10 rounds for AES-128). The final ciphertext C is obtained after the last round of transformations.
Decryption (AES): The decryption process is the inverse of encryption:

1. InverseShiftRows: The rows of the ciphertext matrix are shifted back.
2. InverseSubBytes: The bytes are substituted using the inverse S-box.
3. InverseMixColumns: The linear transformation is reversed.
4. AddRoundKey: The ciphertext is XORed with the corresponding round keys in reverse order to recover the original data.

The decrypted plaintext is obtained after all the rounds.

4.3 Hybrid encryption model

The hybrid cryptosystem combines OU for secure key exchange and AES for bulk data encryption. Below is the mathematical formulation for the entire encryption and decryption process in the hybrid model:
Encryption Process

1. AES Key Generation:
   - A random AES symmetric key K_{AES} is generated: $K_{AES} \in Z^*_{2^128}$
2. AES Data Encryption:
   - The plaintext data P is encrypted using the AES key K_{AES} : $C_{AES} = AES_{Encrypt}(P, K_{AES})$
   - C_{AES} represents the ciphertext of the data.
3. OU Encryption of AES Key:
   - o The AES key KAES is encrypted using the recipient's OU public key (n,g):
     $C_{OU} = g^{k_AES} r^n \bmod n$
     C_{OU} represents the encrypted AES key.

Decryption Process:

OU Decryption of AES Key:

- The recipient uses their private key p to decrypt the AES key K_{AES} from the OU ciphertext C_{OU}:

$$K_{AES} = \frac{L(c_{ou}^{(p-1)} \bmod p^2)}{(L(g^{(p-1)} \bmod p^2))} \bmod p$$

1. AES Data Decryption:
   - The decrypted AES key K_{AES} is used to decrypt the AES-encrypted ciphertext C_{AES} to retrieve the plaintext P:

$$P = AES_{Decrypt}(C_{AES}, K_{AES})$$

4.4 Security analysis

The hybrid cryptosystem relies on the security properties of both OU and AES:

- **OU Security:** Namely, the security of OU is easy to achieve since the time to factor $[n = p2q]$ is very hard compared to the protection offered during key exchanges.
- **AES Security:** AES is immune to most contemplated attacks such as brute force attacks, differential attacks, and linear attacks, because of its large key length and multiple linguistic processing.

This section presents an analysis on performance analysis with the help of experimental results of the implementation of Okamoto-Uchiyama (OU) + AES hybrid cryptosystem. The calculations are kept to encryption time, decryption time and system overheads. These values are compared to similar systems which have been described in some of the above references.

- AES encryption key size: 128 bits
- AES block size: 128 bits (large-scale data typical choice for data encryption and decryption)
- Dataset size: One gigabyte potency; the ideal overall size of the cloud dataset.
- Cloud environment: I utilised a virtualized cloud server with Azure that supports modern forms of hardware like Intel Xeon processors.

Encryption Time: Encryption time is the number of times it takes to encrypt a given dataset. For the proposed hybrid system, the encryption is now divided into (AES encryption for most of the data and OU encryption for the AES key exchange). Proposed Hybrid System (OU + AES):

1. AES encryption time for 1 GB dataset:
   AES encryption throughput is high, with such an average throughput of 500 MB/s in modern cloud environments. Again, Encryption Time = 1 GB/500MB/s = 2 seconds
2. OU encryption time for AES key: The AES key (128-bit) is encrypted using OU cryptosystem. The OU public key encryption is more computational than AES, but as only the AES key, a small amount of data is encrypted it takes negligible time. In modern hardware, the OU encryption time for the AES key is close to 10 ms (milliseconds). 3. Total encryption time for the proposed hybrid system: Total Encryption Time = 2002 ms Total Encryption Time as in bits = 2.01 seconds.
   The amount of work required to encrypt and exchange keys is computed by system overhead. Proposed Hybrid System (OU + AES):
   - Overhead: Low. It adapts to the least usage of computational assets, which enhances its flexibility when implemented in cloud settings with a massive number of users.
3. RSA + AES System
   RSA comes with the aspect of introducing higher computational costs when establishing intended keys.
   - Overhead: Moderate. RSA key exchange is more expensive than OU.
4. Paillier + RSA System [6]:
   Paillier and RSA are both types of asymmetric encryption algorithms to incorporate which incur higher overhead.
   - Overhead: High. This system utilises relatively higher computing power, especially in large cloud environments.

In comparing the proposed Okamoto-Uchiyama (OU) + AES hybrid cryptosystem with other references in cloud security & hybrid cryptography, additional references discussing hybrid cryptosystems using combinations of RSA, AES, Paillier, NTRUEncrypt and other, performance metrics will be included. Table 1 show below presents a comparison of our work with other related work in terms of encryption time, decryption time, system overhead and scalability.

Encryption Time: The use of AES in performing the bulk encryption for the proposed model also makes it very efficient. They have been tested to be very fast with 2.01 seconds a 1GB dataset. The additional overhead incurred by the OU encryption of the AES key is very small, so key exchange requires only 10 milliseconds.

Decryption Time: Unlike encryption, the decryption results are optimised by using AES, and the decryption of the AES key by OU takes only 10 milliseconds.

Decryption Time: Unlike encryption, the decryption results are optimised by using AES, and the decryption of the AES key by OU takes only 10 milliseconds.

System Overhead: Low system overhead because AES for data encryption and OU for key exchange are well-defined and partitioned.

Scalability: Built to scale in the cloud and capable of dealing with big data spread across multiple servers.

Proposed Hybrid System (OU + AES): As illustrated in the previous figures, this system exhibits the best balance of speed, outgoing overhead, and scalability across all workloads, which makes it quite suitable for cloud applications to perform encryption of large volumes of data and their subsequent secure exchange.

NTRUEncrypt-Based System: While this system is as efficient as the proposed model and offers a similar level of performance, NTRUEncrypt may also add complexity based on the deployment. It is, however, very suitable for large cloud environments. Large cloud environments have a lower risk since the number of interfaces and interconnection likelihood are limited by activities on a sufficient scale.

The results prove that the OU + AES hybrid cryp-

Table 1 Results and Performance Comparison

Metric	Proposed Hybrid System (OU + AES)	RSA + AES System [7, 22]	Paillier + RSA System [6]	NTRUEncrypt-Based System [8]	Hybrid RSA + NTRU [12]
AES Encryption Time (1 GB)	2.00 seconds	2.00 seconds	2.00 seconds	2.00 seconds	2.00 seconds
Key Exchange Encryption Time	10 ms	50 ms	100 ms	15 ms	40 ms
Total Encryption Time	2.01 seconds	2.05 seconds	2.1 seconds	2.015 seconds	2.04 seconds
AES Decryption Time (1 GB)	2.00 seconds	2.00 seconds	2.00 seconds	2.00 seconds	2.00 seconds
Key Exchange Decryption Time	10 ms	50 ms	100 ms	15 ms	40 ms
Total Decryption Time	2.01 seconds	2.05 seconds	2.1 seconds	2.015 seconds	2.04 seconds
System Overhead	Low	Moderate	High	Low	Moderate
Scalability	High	Moderate	Low	High	Moderate
Brute Force Resistance	High	High	High	High	High
MITM Attack Defense	High (OU key exchange)	Moderate	Moderate	High	High

tosystem offers the greatest advantage over the competition in terms of security, scalability, and minimum interference with the system in the modern cloud platform.

5 CONCLUSIONS

The proposed hybrid cryptosystem by incorporating Okamoto-Uchiyama (OU) public key encryption with Advanced Encryption Standard (AES) is efficient enough and a secure access point to meet the overhead objectives of the security layers in the cloud environments. Using OU for key exchange and AES for fast data encryption, the system minimizes the commonly perceived burden of asymmetric encryption and preserves the security factor. From the experimental results, the hybrid model outperforms the RSA cryptographic system in encryption and decryption in large datasets inherent in cloud services. Integrating one of the processes as a lightweight key exchange method using OU means that the additional time taken should be considerably small and would not significantly raise the overall encryption and decryption times, even with the huge data sets. Moreover, the hybrid system also offers considerable protection against most ordinary cryptanalytic attacks, including brute force and MITM attacks, making it the apt security framework for CT Cloud data. Overall, incorporating it into different cloud service types including SaaS, PaaS and IaaS turns its practical usability into another advantage. Compared to other encryption systems such as RSA + AES, Paillier + RSA, and NTRUEncrypt-based, the proposed model exhibits increased efficiency, scalability, and security. The enumerated hybrid model responds not only to the knowledge-focused security requirements of Cloud Computing but also to the performance-related requirement, making both a promising and scalable basis of modern Cloud Services in healthcare, finance, and government apps. In conclusion, the proposed method, OU + AES hybrid cryptosystem for cloud computing provides a secure and feasible approach for secure and rapid data processing without any insecurity or threat originated from the cloud environment. This emerges as a feature for scalability with liberal overhead that can handle the security issues as well as the degradations observed in specific encryption-oriented procedures and protocols.

ACKNOWLEDGEMENT

N/A

FUNDING SOURCE

No funds received.

DECLARATIONS

Conflict of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Consent to publish

All authors consent to the publication of this work.

Ethical approval

Not Applicable

REFERENCES

[1] Ridho A, Tulus, Efendi S. Optimization of The Gronsfeld Cipher Key Using Okamoto-Uchiyama Public-Key Cryptosystem for Data Security. In: 2020 3rd International Conference on Mechanical, Electronics, Computer, and Industrial Technology (MECnIT). IEEE; 2020. p. 123–126. 10.1109/mecnit48290.2020.9166598

[2] Anisha M, Beenu VA. Double secure cloud medical data using Euclidean distance-based Okamoto Uchiyama homomorphic encryption. International Journal of System Design and Computing. 2024;2(01):1-7. https://kitspress.com/journals/ IJSDC/index.php?isuid=9info=15

[3] KAREEM S. Secure Cloud Approach Based on Okamoto-Uchiyama Cryptosystem. Journal of Applied Computer Science & Mathematics. 2020;14(1):9–13. 10.4316/jacsm.202001001

[4] Ismail G, Alhayali S, Kareem S, Hussain Z. Secure Data in the Cloud with a Robust Hybrid Cryptographic Approach. Journal of Electrical Systems. 2024;20(2):2450–2457. 10.52783/jes.2018

[5] Murad SH, Rahouma KH. In: Hybrid Cryptography for Cloud Security: Methodologies and Designs. Springer Singapore; 2021. p. 129–140. 10.1007/978-981-16-2275-5_7

[6] ABDALWAHID SMJ, YOUSIF RZ, KAREEM SW. ENHANCING APPROACH USING HYBRID PAILLER AND RSA FOR INFORMATION SECURITY IN BIGDATA. Applied Computer Science. 2019;15(4):63–74. 10.35784/acs-2019-30

[7] Akter R, Khan MAR, Rahman F, Soheli SJ, Suha NJ. RSA and AES Based Hybrid Encryption Technique for Enhancing Data Security in Cloud Computing. International Journal of Computational and Applied Mathematics & Computer Science. 2023;3:60–71. 10.37394/232028.2023.3.8

[8] Khalid Yousif M, Dallalbashi ZE, Kareem SW. Information security for big data using the NTRUEncrypt method. Measurement: Sensors. 2023;27:100738. 10.1016/j.measen.2023.100738

[9] Abdalwahid SM, Ibrahim BF, Ismael SH, Kareem SW. A New Efficient Method for Information Security in Hadoop. Qalaai Zanist Scientific Journal. 2022;7(2). 10.25212/lfu.qzj.7.2.42

[10] Yousif R, Kareem S, Abdalwahid S. Enhancing approach for information security in Hadoop. Polytechnic Journal. 2020;10(1). 10.25156/ptj.v10n1y2020.pp81-87

[11] Altarawneh K. A Strong Combination of Cryptographic Techniques to Secure Cloud-Hosted Data. Journal of Namibian Studies: History Politics Culture. 2023;33. 10.59670/jns.v33i.727

[12] ALTARAWNEH K, ALTARAWNI I, ALMAIAH M, HAMMAD M, ALKHDOUR T, ALALI R, et al. A HYBRID MODEL OF RSA AND NTRU FOR SECURING OF CLOUD COMPUTING. Journal of Theoretical and Applied Information Technology. 2024;102(7)

[13] Li H, Shi J, Tian Q, Li Z, Fu Y, Shen B, et al. E nc 2 DB: A Hybrid and Adaptive Encrypted Query Processing Framework. In: International Conference on Database Systems for Advanced Applications. Springer; 2024. p. 54-70. 10.1007/978-981-97-5562-2_4

[14] Manicka RM, Kiruba B, Jasmine SJI, Manoj KS. In: A Novel Mechanism in Continuous Intelligence for Mining and Aggregating IoT Sensor Data. Chapman and Hall/CRC; 2023. p. 215–224. 10.1201/9781003226888-16

[15] Erinle Y, Kethepalli Y, Feng Y, Xu J. Sok: Design, Vulnerabilities, and Security Measures of Cryptocurrency Wallets. 2025. 10.2139/ssrn.5237492

[16] Ananthakrishna V, Chandra S. Innovations in Cloud Security: Enhanced Hybrid Encryption Approach with AuthPrivacyChain for Enhanced Scalability. Nanotechnology Perceptions. 2024;20(S2). 10.62441/nano-ntp.v20is2.42

[17] Rakhra M, Singh A, Singh D, Kaur B, et al. Hybrid Cryptography in Cloud Computing. In: 2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO). IEEE; 2024. p. 1-7. 10.1109/ICRITO61523.2024.10522254

[18] Kanakasabapathi RS, Judith JE. Improving cloud security model for web applications using hybrid encryption techniques. International Journal of Internet Technology and Secured Transactions. 2024;13(3):291–308. 10.1504/ijitst.2024.136677

[19] Pothireddy S, Peddisetty N, Yellamma P, Botta G, Gottipati KN. Data security in cloud environment by using hybrid encryption technique: a comprehensive study on enhancing confidentiality and reliability. International Journal of Intelligent Engineering & Systems. 2024;17(2). 10.22266/ijies2024.0430.14

[20] Likhita MSLVS, Ravindranath K, Vaishnavi G, Dabhi V, Teja AS. Hybrid cryptography model to enhance the security in cloud; 2024. EasyChair preprint. https://easychair.org/publications/preprint/95Kg

[21] Reddy KK, Chadha AR, Nikhil PS, Sountharrajan S. Hybrid Cryptography Techniques for Data Security in Cloud Computing. In: 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT). IEEE; 2024. p. 1836–1842. 10.1109/ic2pct60090.2024.10486794

[22] Bhat AN, Kumar R. Efficient Hybrid Encryption Algorithm for Securing Data in Cloud Environment. 2024. 10.21203/rs.3.rs-4233929/v1

[23] Kaleem M, Mushtaq MA, Jamil U, Ramay SA, Khan TA, Patel S, et al. New efficient cryptographic techniques for cloud computing security. Migration Letters. 2024;21(S11):13-28

[24] Maddila SK, Vadlamani N. A Novel Efficient Hybrid Encryption Algorithm Based on Twofish and Key Generation Using Optimization for Ensuring Data Security in Cloud. Journal of Information & Knowledge Management. 2023;23(01). 10.1142/s0219649223500624

[25] Wagh A, Yadav S, Patil P, Magdum S, Shiravale S. Enhanced file storage on Cloud using Hybrid Cryptography Algorithm. In: 2024 3rd International conference on Power Electronics and IoT Applications in Renewable Energy and its Control (PARC). IEEE; 2024. p. 398–404. 10.1109/parc59193.2024.10486514

[26] Akter R, Khan MAR, Rahman F, Soheli SJ, Suha NJ. RSA and AES Based Hybrid Encryption Technique for Enhancing Data Security in Cloud Computing. International Journal of Computational and Applied Mathematics & Computer Science. 2023;3:60–71. 10.37394/232028.2023.3.8

[27] Koppaka AK, Lakshmi VN. An Efficient and Secured Big Data Storage in a Cloud-based Environment Using Hybrid Cryptography Algorithm and Rivest, Shamir, Adleman Algorithm. International Journal of Intelligent Engineering & Systems. 2024;17(1). 10.22266/ijies2024.0229.45

[28] Mohammed ZA, Ali Hussein K. PRC6: Hybrid Lightweight Cipher for Enhanced Cloud Data Security in Parallel Environment. 2024. 10.2139/ssrn.4715364

How to cite this article

Malik A. A hybrid cryptosystem for cloud security: combining Okamoto-Uchiyama and Advanced Encryption Standard for optimized encryption performance. Journal of University of Anbar for Pure Science. 2025; 19(2):221-230. doi:10.37652/juaps.2025.158225.1364