ISSN: 2755-6190

Research Article

Open Access Journal of Artificial Intelligence and Technology

Fully Utilizing Artificial Intelligence to Achieve Hybrid Encryption Resulting from The Combination of Aes and Rsa

Waddah Mallouk

Al-Wataniya Private University, Syria

***Corresponding author**
Waddah Mallouk, Al-Wataniya Private University, Syria.

Received: December 29, 2025; **Accepted:** January 06, 2026; **Published:** January 12, 2026

ABSTRACT

Artificial intelligence has used in many scientific fields fundamentally, but its use in data protection, particularly in encryption and decryption, has been a supportive and auxiliary tool. This research presents a mechanism for using artificial intelligence to perform fully hybrid encryption, eliminating the RSA and AES algorithms entirely and replacing them with multiple neural networks that perform both encryption and decryption. The mechanism for combining the RSA and AES algorithms was studied, taking into account the cipher lengths. The 12-bit AES algorithm is used fifteen times, compared to the 248-bit RSA algorithm once, to obtain the cipher. This is achieved after segmenting the m-message into mi sub- messages. Forty distinct neural network architectures underwent training for English plaintext encryption and decryption operations.

Each network had three characters as input and three ciphers as output. This number of neural networks is used to solve the problem of the number of elements in the training database, as 40 networks were used for encryption alone, and another 40 networks were used for decryption, along with the segmentation and pooling operations. The proposed model was programmed in the MATLAB GUI environment, and the encryption and decryption times required to perform the proposed model were determined and compared with the execution times of the RSA and AES algorithms. Evaluation results showed that the proposed model outperforms RSA in time of encryption while approaching AES encryption speeds. The results also demonstrated that this model outperforms both the RSA and AES algorithms in decryption, demonstrating its fast performance.

Keywords: AI, RSA, AES, Encryption, Decryption, Hybrid, Cipher

Highlights

- Usage AI to encrypt and decrypt message totally
- Time of encryption is equal to time of decryption approximately
- Novel Proposed hybrid model is consisted of 15 times AES with one time RSA

Introduction

Encryption is one of the most important means of protecting data in communications systems from tampering or unauthorized access. Encryption methods are divided into two categories: symmetric encryption algorithms, such as the standard AES algorithm, and asymmetric encryption algorithms, such as the RSA algorithm. In symmetric algorithms, the encryption key is the same during both the encryption and decryption stages, while the encryption key differs from the decryption key in asymmetric algorithms [1]. In another direction, due to the need for more efficient algorithms, hybrid encryption algorithms have become widespread in advanced stages. These algorithms combine a symmetric encryption algorithm with an asymmetric encryption algorithm, with the aim of taking advantage of the advantages of both, symmetric and asymmetric, to accelerate the encryption and decryption processes and enhances degree of security. This ensures the speed of data transmission and protection without taking a relatively long time. However, the hybridization process is limited by the capabilities of the algorithm used in the hybridization process. That sometimes requires the use of advanced software or computer techniques to overcome this limitation and obtain the capabilities of the algorithms used in

Citation: Waddah Mallouk. VFully Utilizing Artificial Intelligence to Achieve Hybrid Encryption Resulting from The Combination of Aes and Rsa. Open Access J Artif Intel Tech. 2026. 2(1): 1-6. DOI: doi.org/10.61440/OAJAIT.2026.v2.19

the hybridization process with the lowest computational cost, by eliminating the limitations and restrictions of the basic algorithms in the hybridization process. On the other hand, artificial intelligence (AI) technologies have spread widely and deeply in many fields and are considered the most prominent and important software and computer technologies of the current era. Hence, the idea of this research, which is summarized in finding a hybrid encryption methodology based on the AES and RSA algorithms, and then finding an artificial intelligence technique that ensures the proposed hybrid encryption methodology works with the least computational costs and programming complexity.

Research Materials and Methods

The research was conducted according to specific steps, starting with a study of hybrid encryption algorithms based on AES and RSA algorithms. It then studied the use of artificial intelligence in encryption and reviewed the hybrid encryption methodology proposed in this research. It then investigated a mechanism to reward the hybrid algorithm with an artificial intelligence network that ensures the benefits of the hybrid process used to encrypt and protect data in a shorter time.

Reference Study

Artificial intelligence (AI) is used in many encryption techniques, particularly in cloud computing security, which offer flexibility, scalability, and cost-efficiency. However, they still face security challenges. AI-powered encryption techniques are being used to solve these challenges. Machine and deep learning techniques are used to enhance encryption efficiency, improving data confidentiality and maintaining its availability [2]. Given the importance and challenge of securing sensitive data, traditional encryption methods are used to protect data during storage and transmission. Symmetric encryption is considered one of the most important solutions for maintaining confidentiality, but it faces limitations related to its computational cost. Therefore, researchers have resorted to combining AI with symmetric encryption to reduce computational costs and make it scalable and applicable in cloud computing environments.

AI-powered symmetric encryption improves the efficiency of computational operations by reducing computational bottlenecks and improving the flow and pace of computational processing. AI can provide models that simplify symmetric encryption operations [3]. AI-powered encryption has also been used to protect the financial data of small and medium-sized enterprises (SMEs), which are most vulnerable to breaches, leading to significant financial losses and damage to their reputation. Therefore, AI-powered encryption has been used as an effective solution to enhance financial data protection in companies. Results have shown improvements in data security, making AI- powered encryption an essential tool for SMEs, enabling them to counter security threats and breaches [4]. Blockchain technology (which relies on AI and symmetric encryption) has been used to detect attacks and maintain privacy in Internet of Things (IoT) systems. AI- powered attack detection modules are deployed in Blockchain nodes to ensure high accuracy and minimal delay. Prior to transmission, plaintext data undergoes symmetric encryption. The resulting ciphertext trains neural networks, and the optimized model deploys across blockchain nodes to enable private automated detection. Results have shown that the proposed method reduces training time and achieves high detection accuracy, making it effective for real-world systems [5]. The researchers began by considering that traditional encryption methods suffer from computational inefficiency and vulnerability to attacks, in addition to the challenges they face in key management. Artificial intelligence (AI), particularly machine learning and deep learning algorithms, has been leveraged to use intelligent encryption mechanisms to improve data protection from unauthorized access and enhance computational performance.

Experimental results have shown significant improvements in encryption speed and data integrity while reducing computational costs, ensuring secure and instant communications in telecommunications networks. However, the researcher recommended the need to improve AI-based encryption techniques by integrating multiple encryption algorithms to enhance security, privacy, and data transmission efficiency. Researchers also developed a new data protection model based on the intersection of AI, symmetric encryption, and blockchain, addressing key concerns related to privacy, integrity, and transparency [6,7]. Symmetric encryption allows computational operations to be performed on encrypted data, while blockchain ensures data immutability and transparency. AI-driven security systems autonomously identify cyber threats through advanced pattern recognition. Some research has explored the use of artificial intelligence to improve confidentiality in encryption systems, focusing on four encryption systems: the Advanced Encryption Standard (AES), the RSA algorithm, the learning-with-error algorithm, and the Light Weight Ascon Cipher Family. All of these techniques were reviewed, focusing on areas that benefit from cryptanalysis using advanced artificial neural network structures [8].

The potential for using artificial intelligence in the mathematical operations of these algorithms, such as rotation, S-box, or vertical Boolean functions, was studied, along with a study of neural network applications in encryption. Other research has proposed a hybrid encryption model using AES and RSA to preserve the privacy of sensitive data. This is based on the many challenges facing data related to privacy and confidentiality, and the need for numerous measures to protect data privacy and confidentiality in many companies, especially sensitive user data. A hybrid encryption model based on the AES and RSA algorithms has been proposed to protect data and information from threats and to verify information. This model can transfer data securely, as it was created using multiple algorithms. These algorithms enable the user to select the data to be protected or encrypted for secure storage in the cloud [9]. In addition to relying on the AES and RSA algorithms, this model relies on the multi-layer Perceptron neural network to generate and exchange keys. This model enables increased confidentiality while reducing the time required for implementation. With the development of technology, cloud computing has become a center for sensitive information, exposing it to risks, especially when users access it.

Additionally, numerous users utilize it for diverse purposes. Therefore, data must be protected and made secure to create a safe usage environment. Researchers proposed an analysis of the AES and RSA algorithms to determine their time consumption and degree of complexity [10]. The results proved that using the

AES encryption methodology is the first choice for protecting data stored in computing due to its high speed and performance. Researchers presented a hybrid encryption technique to leverage the power of symmetric and asymmetric encryption to protect data and improve its confidentiality during transmission. The AES and RSA algorithms are the most commonly used to protect data and improve confidentiality during transmission. To strengthen confidentiality, the researchers introduced an integrated encryption methodology combining AES and RSA cryptographic primitives. The AES algorithm is used to encrypt data, while the RSA algorithm is used to encrypt the AES key [11]. This proposed technique has many advantages, such as increased confidentiality, making it more difficult for hackers and attackers. It is also characterized by speed, as it relies on the symmetric and faster AES algorithm. The time required to complete both AES and RSA algorithms of different lengths were also studied. Many researchers also studied artificial intelligence methods and approaches used to support and design encryption models and security protocols, particularly the use of artificial intelligence techniques to perform encryption operations such as Boolean functions, S-box, and pseudo-random number generators [12].

Proposed Hybrid Encryption Methodology

This methodology is based on a consensus between the symmetric AES and asymmetric RSA algorithms. The block size in AES is fixed at 128 bits, while in RSA it varies according to the key length. A key length of 2048 bits was adopted, making the RSA block size less than 2048 bits. Therefore, 15 parallel implementations of the AES algorithm were used, and the results were combined to produce an RSA output of 1920 bits. The encryption/decryption Scheme of our methodology appears in Figure 1. The input to the encryption scheme is the message text M, N bits long, which is divided into subblocks ranging from m1 to mn, where n is the number of subblocks, given by the following equation (1):

$$n = \max[N/128] \quad (1)$$

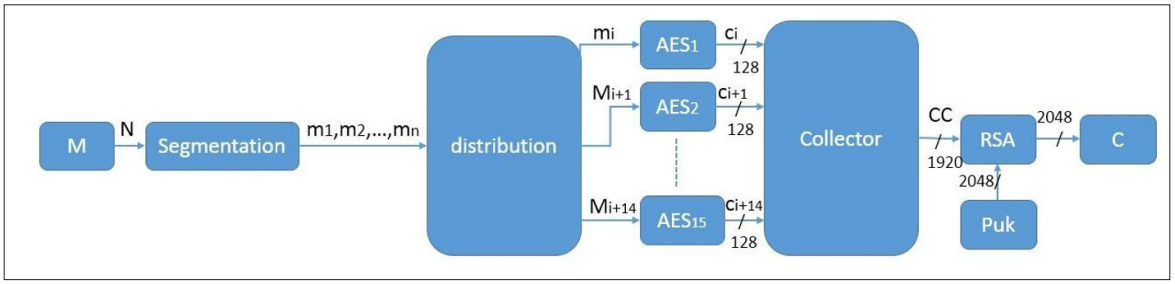
Every 15 blocks are distributed to the AES algorithm to find the corresponding ciphers that are 128 bits long, then these ciphers are collected into one CC cipher that is 1920 bits input is encrypted using the RSA algorithm with 2048-bit key, producing a 2048-bit cipher text C, which is given by the following relation (2):

$$C = (CCe) \bmod n \quad (2)$$

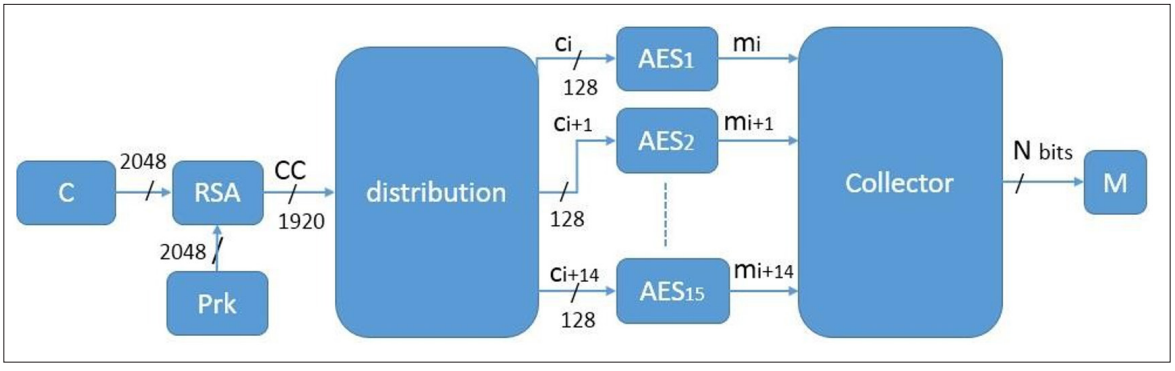
Where e and n are the public key pairs of the RSA algorithm, and on the decryption side, the reverse operations take place, and the cipher C is decrypted according to the following equation (3):

$$CC = (Cd) \bmod n \quad (3)$$

Where d and n are the private key pairs of the RSA algorithm and CC is distributed into sub-ciphers from ci to ci+14 with a length of 128 bits. These ciphers are decrypted using the AES algorithm, so we get the sub-blocks from mi to mi+14, which are assembled to retrieve the message M with a length of N bits.



A- Encryption scheme



B- Decryption Scheme

Figure 1: diagram for the proposed hybrid cryptographic implementation

Hybrid Encryption Using Artificial Intelligence

The number of characters in the message M that can be encrypted according to the hybrid methodology proposed in Figure (1) is calculated as follows:

$$NL = (NAES /240) \quad (4)$$

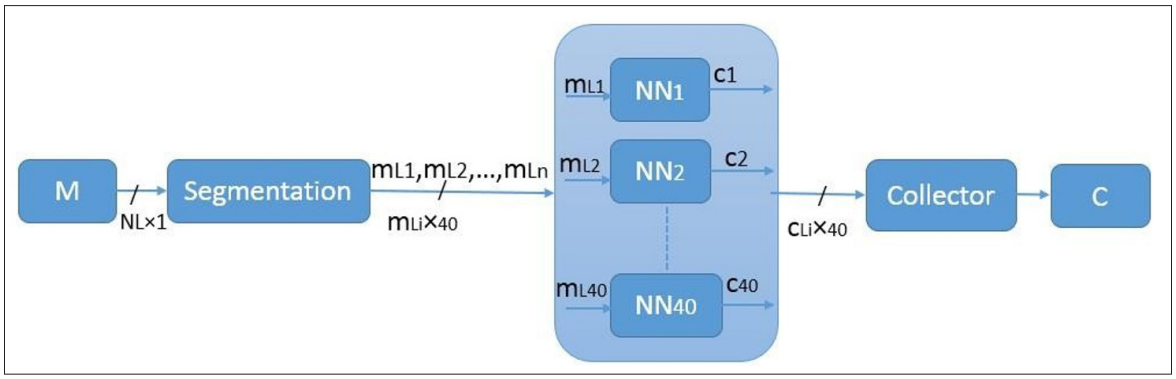
Where:

NL: Number of characters in the message.

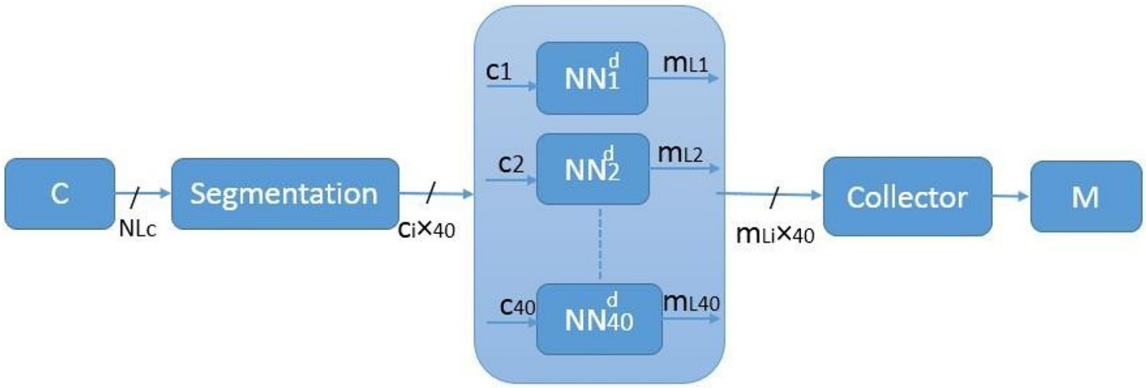
240=15*16: Number of times the AES algorithm is used and16: Unicode characters require 16 bits.

If the number of bits in the AES algorithm is NAES =128, then the number of characters is NL = 120. Therefore, to perform hybrid encryption, we need a neural network with 120

characters as input and the final code as output. To encrypt the English language with its letters in only one case (uppercase or lowercase) with spaces, we need a training database that includes all the possibilities of distributing characters with spaces, which number (1+26)120 which is difficult to implement due to the need for huge memories. The researcher in Reference proposed a solution to this issue by dividing the message into more than one part and distributing these parts to more than one neural network [13]. Therefore, it was suggested to use 40 neural networks. For that reason, the number of database elements was (26+1)120/40 = 19683 characters. Which can be implemented as shown in Figure (2), where the message M is divided into 40 messages mL1, mL40. Then these messages are distributed to the neural networks NN1, … NN40 trained to give the corresponding codes c1…c40 , and these codes are collected to obtain the final code C, while the decoding process is done in reverse, and the neural networks are trained to perform the decoding.



A- Hybrid Encryption Scheme Using Artificial Intelligence



B-Hybrid Decryption Scheme Using Artificial Intelligence Figure (2) System Topology for Ai-Driven Integrated Encryption/ Decryption

Each neural network features two layers with three neurons per layer. The input of the first layer is mLi = [L1 L2 L3]T, while the output of the network (the second layer): ci =[c1 c2 c3] for the NNi encryption network. The public encryption key is the weights of this network: Puki = [W(1)iE W(2)iE] The same applies to the NNiD decryption network, but the input is ci and the output is mLi where: i = 1, 2, 3, 40 and the private key is: Prki = [W(1)iD W(2)iD]

Results and Discussion

The MATLAB GUI (Graphical User Interface) environment was used to program the proposed hybrid encryption using artificial intelligence, as shown in Figure (3). The message text M=”waddah” is entered, then the “Encrypt” button is pressed. The hybrid encryption is executed using artificial intelligence, as shown in Figure (a2). Thus, we obtain the code: C = 22 17 8

19 14 15. When decrypting, the “Decrypt” button is pressed, and the hybrid decryption is executed using artificial intelligence, as shown in Figure 2b. The original message is then retrieved.

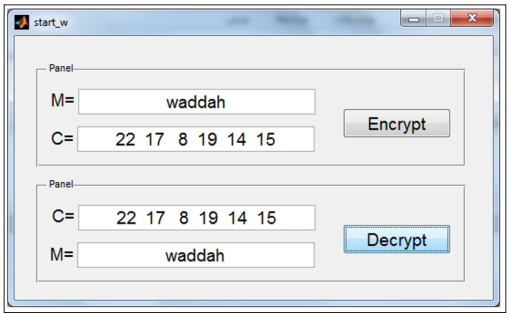


Figure 3: The Proposed Hybrid Encryption Model Using Artificial Intelligence

The proposed AI-based hybrid encryption model was tested and compared with the performance of both the RSA and AES

algorithms. Four text blocks of sizes: 50KB, 100KB, 150KB, and 200KB, were encrypted, and the encryption and decryption times for each block were calculated using the proposed encryption methodology and the RSA and AES algorithms, respectively. Figures (4) and (5) show the encryption and decryption times for these text blocks using the proposed encryption methodology and the RSA and AES algorithms. Comparing the hybrid encryption time using the proposed AI with the encryption times using the RSA and AES algorithms reveals that the proposed model outperforms the RSA algorithm in terms of encryption time. Its encryption time is close to that of the AES algorithm, but it is more secure and protected. The superiority of this model over the RSA algorithm is due to its use of faster mathematical operations than the mathematical operations required to implement the RSA algorithm.

Neural networks rely primarily on multiplication and addition, while the RSA algorithm relies on repeated multiplication (exponentiation operations) and finding remainders, which require much longer times than multiplication and addition. A comparison of the decryption times reveals that the proposed model outperforms both the RSA and AES algorithms. This is due to the fact that the decryption time in the proposed model is close to the encryption time, as the mathematical operations required for encryption are the same as those required for decryption. As shown in Figure (2), the neural structure of both the encryption and decryption schemes is the same in terms of the number of neurons used. Therefore, Decryption requires an identical count of computational operations for encryption. Therefore, the proposed model outperforms both the RSA and AES algorithms, which require the inverse operations necessary for encryption before decryption. These computational processes frequently exhibit extended execution durations.

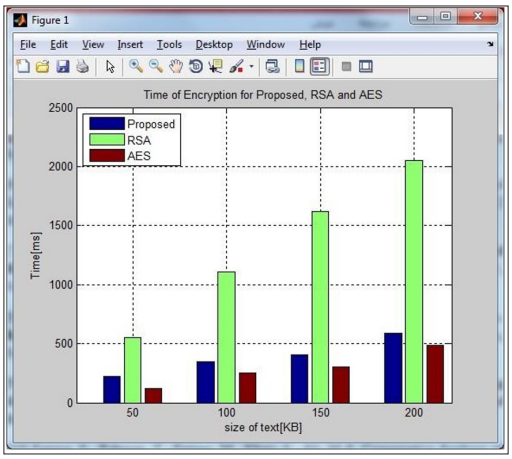


Figure 4: Encryption Times for Different Sized Text Blocks Using the Proposed Encryption Model, The Rsa Algorithm, And the Aes Algorithm.

Summary and Conclusion

Using AI to perform hybrid encryption based on the RSA and AES algorithms reduces encryption and decryption time while maintaining the level of security provided by the hybrid encryption model. This is because AI uses mathematical operations that require less time than those required to program the hybrid model and the RSA and AES algorithms. Using AI in hybrid encryption also demonstrated high efficiency in decryption, requiring approximately the same time as encryption because it uses the same mathematical operations for both encryption and decryption. The encryption and decryption processes are determined by the data used to train the neural network. When the network is trained with the message as its input and the ciphertext as its output, we obtain weights that enable the network to perform encryption. When the network is trained with the cipher (ci) as its input and the message or data (mLi) as its output, we obtain a neural network that performs decryption. However, the structure remains the same, resulting in similar encryption and decryption times when AI is used to perform the proposed hybrid encryption.

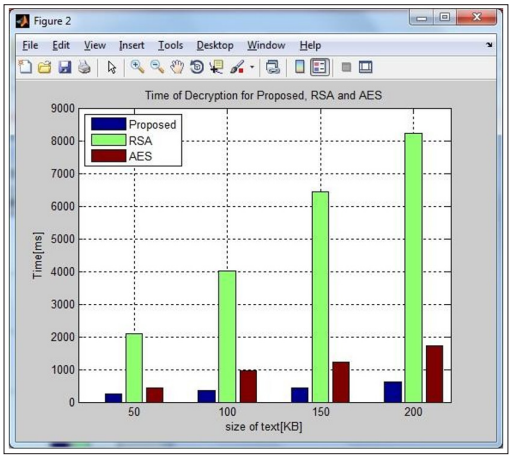


Figure 5: Decryption Times for Different Sized Text Blocks Using the Proposed Encryption Model, The Rsa Algorithm, And the Aes Algorithm.

References

1. Nico P. “Symmetric and asymmetric encryption explained: RSA vs. AES”, Blog. 2025.
2. Mason Mia, Liam Ava. A Comparative Analysis of AI-Driven Encryption Techniques for Hybrid Cloud Security, Federal University of Technology Minna. 2025.
3. Noah Isabella, Ethan Emma, AI-Powered Homomorphic Encryption: Revolutionizing Secure Data Processing in Cloud Environments, Federal University of Technology Minna. 2025.
4. Tesco Eric, Walmart Alice. Fortifying Financial Data: The Efficacy of AI- Powered Encryption for Small and Medium-Sized Businesses, Australian Catholic University, Umm al-Qura University. 2025.
5. Bui Duc Manh, Chi-Hieu Nguyen, Dinh Thai Hoang, Diep Nguyen N, Ming Zeng, et al. Privacy-Preserving Cyberattack Detection in Block chain- Based IoT Systems Using AI and Homomorphic Encryption. 2024.
6. Shiva Kiran Lingishetty, Chandrashekhar Moharir, Mrinal Kumar. AI-Based Encryption Techniques for Securing Data Transmission in Telecommunication Systems. 2025.
7. Benjamin Amelia, Matthew Charlotte. The Intersection of AI, Blockchain, and Homomorphic Encryption: A New Paradigm for Data Security, Federal University of Technology Minna. 2025.
8. Abderrahmane Nitaj, Tajjeeddine Rachidi. Applications of Neural Network- Based AI in Cryptography, Normandie Univ, UNICAEN, CNRS, LMNO, 14000 Caen, France. 2023.
9. Satish Basapur B, Shylaja BS, Venkatesh A. Hybrid Cryptographic Model Using AES and RSA for Sensitive

Data Privacy Preserving, Webology, Special Issue on Current Trends in Management and Information Technology. 2021. 18.

10. Fatima S, Rehman T, Fatima M, Khan S, Ali MA. Comparative Analysis of Aes and Rsa Algorithms for Data Security in Cloud Computing. Eng. Proc. 2022. 20: 14.
11. Venkata Mahesh Babu Batta, Suresh Kumar LK, RSA-AES Hybrid Encryption: Combining the Strengths of Two Powerful Algorithms for Enhanced Securty, IJRAR. 2023. 2.
12. Luca Mariot, Domagoj Jakobovic, Thomas Bäck, Julio Hernandez-Castro. Artificial Intelligence for the Design of Symmetric Cryptographic Primitives, the final publication is available at Springer via. 2022.
13. Mohammad Taha Kafarnawi. Asymmetric Encryption Method Proposed for Arabic Letters Using Artificial Neural Networks, Journal of King Faisal University: Basic and Applied Sciences No 2-year. 2021.