

Enhancing data security using a multi-layer encryption system

Osama Abd Qasim¹, Sajjad Golshannavaz²

¹Computer Engineering Department, Faculty of Electrical and Computer Engineering, Urmia University, Urmia, Iran

²Electrical Engineering Department, Faculty of Electrical and Computer Engineering, Urmia University, Urmia, Iran

Article Info

Article history:

Received Jun 4, 2024

Revised Oct 4, 2024

Accepted Oct 23, 2024

Keywords:

Advanced encryption

Advanced encryption standard

Decryption

Digital dictionary

Encryption

Rivest-Shamir-Adleman

ABSTRACT

This study highlights the interesting potential of a new multilayer cryptography scheme for reliable data protection in the field of cybersecurity. To do so, an intensive examination of a multi-layer encryption mechanism is proposed to reinforce the defenses in opposition to online threats to touchy data. The strategy is multilevel, with a superior digital dictionary serving as the foundation for the primary layer. The laborious procedures that went into making this dictionary, including rotation differences, ASCII conversion, and chaotic matrix era, upload to its encoding trouble. A modified model of the advanced encryption standard (AES) algorithm with a brand-new key generation technique, which is based on the chaos idea is furnished through layer 2. A parameter is encrypted using the Rivest-Shamir-Adleman (RSA) method, and further precautions are taken to assure the security of the encryption key. When it comes to encryption time, the first layer significantly outperforms the AES method. In addition to exhibiting instantaneous efficiency in data protection, the first layer outperformed the AES algorithm in terms of encryption time which took more than 3 seconds, and the first layer took less than 0.01 seconds, while both approaches functioned identically in terms of information decryption. In-depth talks are given to customize the suggested method's performance. The results demonstrate the effectiveness of the suggested multi-stage encryption and decryption system and demonstrate its efficacy in protecting text documents.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Sajjad Golshannavaz

Department of Electrical Engineering, Faculty of Electrical and Computer Engineering, Urmia University
Nazlo Campus, 11th km, Sero Road, Urmia, West Azerbaijan, Iran

Email: s.golshannavaz@urmia.ac.ir

1. INTRODUCTION

It is now essential to protect private and sensitive information from cyber threats due to the quick development of technology and the younger generation. As attack complexity increases, it will be crucial to develop strong cryptography systems that can protect private information from unauthorized access. To address this demand and improve sensitive data security, this research suggests a multilayer encryption method. Text data is protected by first and second-layer encryption algorithms, and the efficacy of each strategy is assessed using a variety of analytical tools [1].

The devised encryption scheme's first layer uses a logo-new virtual dictionary that makes an effort to duplicate the plaintext the usage of diverse letters and emblems [2]. This innovative method improves the security of sensitive data, strengthening the encryption process overall. In addition to dividing the numerical values into higher and lower dimensions and sorting the higher values, the suggested digital dictionary also converts the ciphertext characters to ASCII format and dynamically adjusts the lower values to suit the demands of the sender and recipient. It modifies parameters in a very methodical manner. The ciphertext,

which serves as a strong basis for the initial step of the cryptographic process, is created by converting the resulting transformed integers to characters [3].

The second version of the advanced encryption standard (AES) algorithm [4] for cryptographic systems has been modified and optimized to improve the performance of second-layer encryption. The 192-bit encryption key generated by chaos theory is an integral part of this layer. The proposed method uses a collection of weak parameters with a value of less than 1 to store the encryption key. To further enhance security, every value necessary for primary generation is shared by the sender and receiver, except one. This special parameter is sent together with the Rivest-Shamir-Adleman (RSA) encrypted ciphertext. The encrypted data can then be successfully decrypted by the client side regenerating the encryption key in the second layer of the system [5].

This paper offers a thorough evaluation of the cautioned multi-layer encryption scheme based on clarifying the specifics of each layer. By combining modern-day AES set of rules modifications with digital dictionary methods, the gadget aims at creating robust and dependable protection against cyber threats, making sure the best level of protection for touchy and vital data is achieved [6]. This study is organized as follows: a review of prior research on this topic is done in section 2. Section 3 explains the methodology, standards, and algorithms used in the study. In section 4, the values of the suggested criteria and standards are provided and discussed together with the experimental and processing algorithm findings. In section 5, outcomes are addressed and assessed. Section 6 clarifies the obtained the result.

2. LITERATURE REVIEW

A recent study on attribute-based encryption (ABE) is done by researchers, aims at securing data sharing with restricted access based on user attributes and keeping data contents safe from unauthorized access [7]. To solve the issues with the ABE cipher text key policy's execution time, they suggested the hybrid ABE cipher text key policy (HCKP-ABE) [8] approach. In scenarios where precise access control and secure data interchange are necessary, especially when there are fewer users in relation to the features, the suggested HCKP-ABE outperforms current systems in terms of key size (512 bits) and execution time (0.0189 s). The study includes a thorough implementation analysis as well as a system-by-system comparison of AES, RSA, and KP-ABE. The potential to create a novel encryption method using the AES algorithm to create fast and real-time text data protection served as the impetus for this investigation.

Seeking to improve the safety of file storage, Betrand *et al.* [9] have developed a hybrid encryption method and discussed the safety troubles with cloud-based large data garages. This system employs the rapid application development (RAD) methodology to put in force each symmetric (AES) and asymmetric (RSA) encryption. A hybrid cryptography device was built which confirmed quick performance and robust security through checking out and evaluation. Other hazards, in the meantime, have been considered, including the incapacity to prepare data within online applications and larger documents following encryption. Despite these drawbacks, the proposed technique drastically increases the safety of cloud-primarily based document storage and increases facts security and confidentiality within the cloud surroundings.

The method proposed in [10] addresses safety issues in cloud-primarily-based massive data storage and gives a hybrid encryption technique to enhance text file storage and report protection. This device employs the rapid application development (RAD) technique to put into effect both symmetric (AES) and asymmetric (RSA) encryption methods. A hybrid cryptography gadget that was constructed using PHP, JavaScript, and Laravel confirmed quick performance and sturdy safety through trying out and assessment. Other dangers, meanwhile, have been reported, consisting of the disability to set up records inside online packages and larger files following encryption. Despite these drawbacks, the counseled method significantly raised the safety of cloud-primarily-based file storage and increased statistics safety and confidentiality in the cloud environment. The counseled device performs better than current models in terms of overall performance, dependability, and stable communicate, according to test findings [11].

Giwa *et al.* [12] have proposed a hybrid method to deal with vulnerabilities in popular encryption algorithms like AES and RSA which might be at risk of brute pressure attacks. The hybrid system combines honeycomb encryption (HE) with a residue-wide variety scheme. Using a distribution transformation decoder based on the Chinese rest principle (CRT) and HE generation, the gadget produces the keys with the usage of a traditional module array and decrypts the statistics. The proposed approach targets storing processing time and enhances protection utilizing generating fake records when an attacker tries to get entry using a wager key which is the same as the real key. According to experimental statistics, the machine has faster processing speeds and is more resilient to brute-force assaults than previous systems. By taken into consideration all these matters work proposes a secure and powerful approach to hybrid encryption. Based on this approach, a unique hybrid technique is proposed that boosts safety, decreases processing time, and resolves some of the shortcomings of traditional cryptographic algorithms.

The papers investigated all cope with security-associated subjects in loads of contexts, together with cloud computing and statistics switches. Systems that use hybrid cryptography are recommended as an effective approach to enhance protection [13]. These merging methods can be symmetric and asymmetric. Modern techniques like honey encryption (HE), quantum key distribution (QKD), and residual numbering may lessen vulnerabilities, particularly when confronted with brute force attacks. The findings inspire a similar look to hybrid encryption strategies and actual global applications to beautify records and data safety and integrity. Besides, a good protection against threats is verified.

3. METHOD

As clarified so far, development and assessment of a multi-layer encryption system that sufficiently shields private statistics data from online attacks, is the milestone of this study. The recommended approach is split into sections, every one of which will increase data protection with the aid of utilizing a powerful encryption mechanism. To facilitate in selecting the most effective option, this examination presents a greater thorough evaluation of several textual content file encryption techniques. Data is dispersed randomly while it is encrypted. In this special approach, the encryption keys should be owned by both the sender and the recipient. Using the encryption key, the encryption technique is reversed all through decryption to get better and unique statistics content material [14].

3.1. Proposed digital dictionary

A present-edge digital dictionary is incorporated into the cautioned multi-layer encryption system to enhance the protection of sensitive data in opposition to net threats. This novel lexicon is built with the use of a meticulously notion-out five-step system. First, each character is translated inside the ciphertext into ASCII layout, in which a two-digit variety corresponds to every individual [15]. The advent of a chaotic matrix with parameters that can be determined via the sender and recipient is the idea of this encryption. Next, the 2-digit quantity is meticulously cut up into its pinnacle and bottom halves. Because it serves as a set reference point, an excessive quantity stabilizes the encryption method. The subsequent level within the crypto method is to rotate the lower integers left and right whilst accounting for the values encoded in the chaos map. The encryption turns into more state-of-the-art and complicated as a result of this rotation being accomplished in numerous instances and the result optimized [16]. The term “chaotic matrix era” describes the time frame in which encryption is achieved by generating a matrix using chaotic theory. “Rotation differences” are the result of changing text characters' ASCII values according to values in a chaotic matrix.

The ciphertext is formed when the newly converted digital values are smoothly transferred into characters at the end of this process. The protection of critical data is improved by this dynamic and intelligent approach to encryption, which guarantees a higher level of sophistication as in Figure 1. The suggested digital dictionary is the cornerstone of multi-layered protection against cyber threats, offering a robust shield for sensitive and important data by fusing mathematical precision with chaotic dynamics [17]. The following is the pseudo-code [18] of key creation and the encryption procedure; for de-coding, the stages are reversed. Coherent encryption is ensured by switching from the digital dictionary to the modified AES algorithm. Using a digital dictionary to alter the text, we then produce dynamic AES keys for strong encryption.

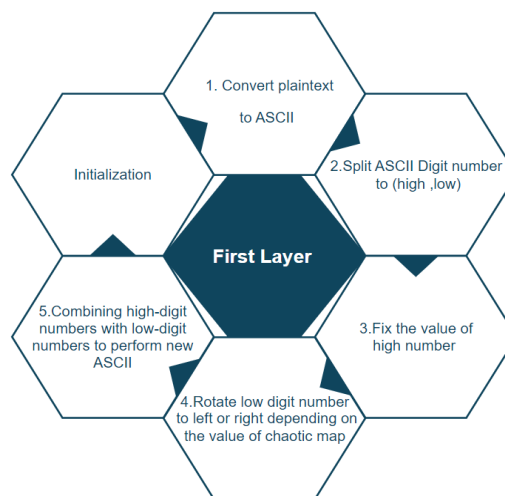


Figure 1. The first layer encryption

- Step 0: Setup
Put the key and *chaotic_matrix* to none.
- Step 1: generation of keys
construct the encryption key, use the *create_key()* method.
- Step 2: The process of encryption
Call the function encrypt (plaintext, key).
Transform ASCII to plaintext.
Use a chaotic matrix to process ASCII values.
Convert updated ASCII values to create the ciphertext.
- Step 3: The decoding process (the encryption reversed) is done.
by using the decode (ciphertext, key) function.
- Step 4: Use case illustration
- Step 5: Create a key for encryption.
- Step 6: To obtain ciphertext, encrypt the plaintext.

3.2. Advanced encryption standard

A well accepted symmetric block cipher with a reputation for flexibility and security is the advanced encryption standard (AES). Unlike Feistel ciphers, the recursive structure employed in AES is based on Substitution permutation networks (SPN). Using several mathematical operations carried out by block cipher algorithms, this network guarantees strong encryption and decoding's works on byte arrays, but plain text is stored in fixed 128-bit blocks that are organized in a 4×4 grid [19]. Multiplication by the key length determines the number of rounds in which AES is executed, which is a basic feature of the algorithm. AES adjusts its rounds proportionately, utilizing 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys [20]. The three key sizes are 128, 192, and 256-bit each. Its success in offering a strong defense against cyber threats is demonstrated by the widespread use of this algorithm in hardware and software worldwide as in Figure 2. It has been discovered that the absence of evidence of hacking against the security of AES [21]. The following is the pseudocode used in the encryption and key creation processes: The phases are inverted for decoding.

- a. Start
- b. Key making process
- c. Create a public key
- d. Make a private key.
- e. Procedure of encryption
- f. Public key is (i, m) or I is for public
- g. $CF = (M \wedge i) \text{ mod } (m)$
- h. There is encrypted data in the packet
- i. Stop.

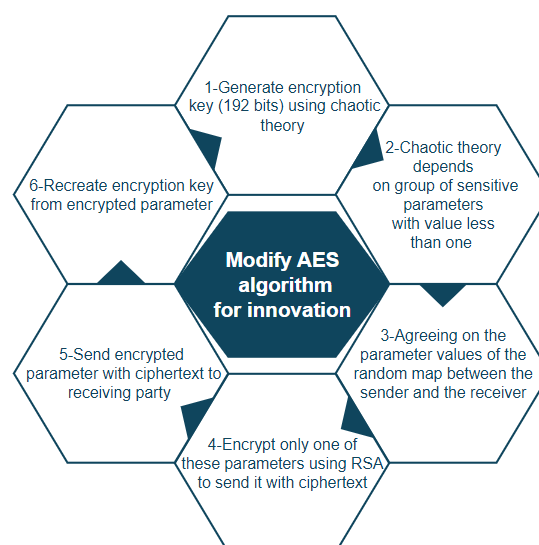


Figure 2. The second layer encryption

3.3. Computational execution time

The efficiency of the method is determined in part by how quickly data is encrypted and decrypted. The system's dependability and security improve when the algorithm completes its tasks in real-time. After 10 successive tries to yield steady results, the elapsed execution time is computed and the execution time is balanced [22]. In this context, execution time encompasses a thorough evaluation of multiple criteria that indicates the effectiveness and general functioning of the cryptosystem. The goal of this approach is to balance multi-layer encryption while increasing task processing time at various levels [23]. As the mathematical model below:

$$T_{\text{exec}} = \frac{1}{10} \sum_{i=1}^{10} (T_{\text{encrypt},i} + T_{\text{decrypt},i}) \quad (1)$$

4. EXPERIMENTAL RESULT AND DISCUSSION

The quality of encryption is checked by calculating the area of the text file before and after encryption to determine the extent to which the file size changes after withdrawing the ciphertext data and the key. The closer the file size after encryption is to the file size of the plaintext, the higher the encryption quality, and the decryption process is consistent with the encryption processes [24]. This issue is outlined in Table 1.

It is seen that the file's size remains unchanged and returns to its initial size once the decryption procedure is complete. It may be concluded that the encryption layers are constant in their levels and stages. In addition to reversing the encryption process to recover the original text is totally right [5].

The computer specifications used are:

- Hard disk capacity: 1 TB
- Operating system: Windows 11
- Processor model: Core i7 11th generation
- Graphics processing unit (GPU): NVIDIA RTX
- Random access memory (RAM) size: 16 GB

Table 1. Text file and size management by encryption and decryption processes

Plain text file	Cipher text file	Decipher text file
144 Bytes	144 Bytes	144 Bytes

4.1. Computational execution time

The average time for key generation and suggested dictionary operations are shown in Table 2. According to a broad range, the AES algorithm performs faster in the encryption and decryption procedures than the RSA method [25]. Based on the results in Table 2 and Table 3, it is concluded that the computational time per second and milli-second encryption for the proposed dictionary is faster than for the AES.

The average elapsed time should be put under investigation in numerical analysis. To this end, the decryption process needs to be completed. As shown in Table 4, it is noticed that the average elapsed time in seconds and milliseconds for both the AES algorithm and the dictionary are very close.

According to the suggested algorithms, numerical simulations, and studies, the multi-level encryption and decryption process successfully encrypts text files in 0.01 seconds. The first level of the suggested method outperforms the AES algorithm in terms of encryption time, which took more than 3 sec. Regarding the decryption procedure, both exhibit a very similar rate of elapsed time.

Table 2. Computational time for key generation and dictionary

Attempt Number	Key generation time (s)	Dictionary time (s)
1	0.00047	0.000009
2	0.00057	0.000015
3	0.00013	0.000010
4	0.00047	0.000009
5	0.00010	0.000008
6	0.00010	0.000009
7	0.00010	0.000009
8	0.00009	0.000010
9	0.00022	0.000641
10	0.00009	0.000008
Computational time (s)	0.00023	0.00007
Computational time (ms)	0.237 ms	0.073 ms

Table 3. Computational time per second for AES encryption

AES encryption time (one block)	Total encryption time (s)
0.0040	0.0040
0.0027	0.0027
0.0026	0.0026
0.0025	0.0025
0.0023	0.0023
0.0025	0.0025
0.0023	0.0023
0.0029	0.0029
0.0023	0.0023
0.0029	0.0029
Computational (0.00274)	Computational (0.00275)
Total (2.748 ms)	Total (2.754 ms)

Table 4. Computational time per second for AES and dictionary decryption

Dictionary decryption time (s)	AES decryption time (s)	Total decryption time (s)
0.0002275	0.00153	0.00176
0.0000089	0.00046	0.00047
0.0000096	0.00026	0.00027
0.0000085	0.00029	0.00029
0.0000083	0.00027	0.00028
0.0000076	0.00028	0.00029
0.0000076	0.00029	0.00030
0.000008	0.00028	0.00029
0.0000109	0.00029	0.00030
0.0000078	0.00029	0.00029
Computational 0.00003 (s)	Computational (s) 0.00042	Computational (s) 0.00045
Computational 0.0304 (ms)	Computational 0.429 ms	Computational 0.459 ms

5. CONCLUSION

A strong encryption method was created to protect private data from internet threats. In the first layer of the proposed multi-layer technique, a new digital dictionary was constructed, and various processes such as ASCII conversion, chaotic matrix generation, and rotational transformations were used to raise the coding complexity. To guarantee key confidentiality and provide unique keys based on chaos theory, the second layer offered a modified version of the AES algorithm based on the RSA method. It is evident from the discussion that the multi-level encryption and decryption procedure successfully secures text files. In comparison to the AES algorithm, the first layer demonstrated better encryption time at 0.01 seconds efficiency than the AES algorithm which took more than 3 seconds, demonstrating its instant efficiency in data protection. Both approaches displayed similar elapsed periods during the decoding process, suggesting that at this stage their levels were similar. This effective multi-layer encryption implementation is a viable strategy for strong data protection against cyberattacks.




REFERENCES

- [1] C. Manthiramoorthy, K. M. S. Khan, and N. A. A. "Comparing several encrypted cloud storage platforms," *International Journal of Mathematics, Statistics, and Computer Science*, vol. 2, pp. 44–62, Aug. 2023, doi: 10.59543/ijmscs.v2i.7971.
- [2] S. A. R. Shirazi, A. Wahab, S. A. Shah, A. Anwar, R. Akhtar, and N. Yousaf, "Quantum shield for IoT: Enhancing Bluetooth security with a novel hybrid encryption algorithm," *The Asian Bulletin of Big Data Management*, vol. 4, no. 1, Feb. 2024, doi: 10.62019/abbdm.v4i1.91.
- [3] X. Zhang and F. Zhou, "An encoding table corresponding to ASCII codes for DNA data storage and a new error correction method HMSA," *IEEE Transactions on Nanobioscience*, vol. 23, no. 2, pp. 344–354, Apr. 2024, doi: 10.1109/TNB.2024.3356522.
- [4] N. A. Ariffin Mohd and A. Y. Ahmed Ashawesh, "Enhanced AES algorithm based on 14 rounds in securing data and minimizing processing time," *Journal of Physics: Conference Series*, vol. 1793, no. 1, Feb. 2021, doi: 10.1088/1742-6596/1793/1/012066.
- [5] M. Y. Shakor, M. I. Khaleel, M. Safran, S. Alfarhood, and M. Zhu, "Dynamic AES encryption and blockchain key management: A novel solution for cloud data security," *IEEE Access*, vol. 12, pp. 26334–26343, 2024, doi: 10.1109/ACCESS.2024.3351119.
- [6] K. Iqbal, M. U. Jatoi, M. Sulaman, and M. S. Abid, "Robust multi-party computation in critical infrastructure protection using hybrid RSA-AES algorithm for enhanced security," Jan. 2024, doi: 10.21203/rs.3.rs-3884946/v1.
- [7] A. S. S. Rani, K. Rohini, K. Pavani, J. R. S. Sree, T. P. Kumar, and P. Yellamma, "Hybrid cipher-text key policy attribute-based encryption (HCKP-ABE): The performance analysis and scalability in virtual machines," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 19, pp. 460–470, 2024.
- [8] W. Wang, R. Liu, and S. Cheng, "Privacy protection of communication networks using fully homomorphic encryption based on network slicing and attributes," *Scientific Reports*, vol. 14, no. 1, pp. 1–18, Aug. 2024, doi: 10.1038/s41598-024-69501-5.
- [9] C. U. Betrand, C. G. Onukwughu, M. E. Benson-Emenike, C. ifeanyi Ofoegbu, and N. M. Awaji, "File storage security in cloud computing using hybrid encryption," *Internet of Things and Cloud Computing*, Jan. 2024, doi: 10.11648/j.iotcc.20241201.11.




- [10] Anirudha, B. P. Sahu, Chirag, V. Pillai, and N. C. Gowda, "Design and development of peer-to-peer distributed computing and storage," in *AIP Conference Proceedings*, AIP Publishing, 2024, doi: 10.1063/5.0184288.
- [11] J. Sivakumar and S. Ganapathy, "An effective data security mechanism for secured data communications using hybrid cryptographic technique and quantum key distribution," *Wireless Personal Communications*, vol. 133, no. 3, pp. 1373–1396, Dec. 2023, doi: 10.1007/s11277-023-10813-6.
- [12] T. A. Giwa, O. I. Abiodun, A. E. Omolara, and R. M. Isiaka, "A hybridized honey encryption for data security using residue number system," *International Journal of Information Security and Cybercrime*, vol. 12, no. 2, pp. 9–22, Dec. 2023, doi: 10.19107/ijisc.2023.02.01.
- [13] M. Alhayani and M. Al-Khiza'ay, "Analyze symmetric and asymmetric encryption techniques by securing facial recognition system," in *Lecture Notes on Data Engineering and Communications Technologies*, vol. 147, Springer International Publishing, 2023, pp. 97–105, doi: 10.1007/978-3-031-15191-0_10.
- [14] R. K. Gupta, H. S. Lamkuche, and S. Prasad, "Enhancing the security of sensitive data in cloud using enhanced cryptographic scheme," in *Studies in Systems, Decision and Control*, vol. 503, Springer Nature Switzerland, 2024, pp. 387–399, doi: 10.1007/978-3-031-43490-7_29.
- [15] Y. Li, H. Yu, B. Song, and J. Chen, "Image encryption based on a single-round dictionary and chaotic sequences in cloud computing," *Concurrency and Computation: Practice and Experience*, vol. 33, no. 7, Mar. 2021, doi: 10.1002/cpe.5182.
- [16] M. Alhayani, N. Alallaq, and M. Al-Khiza'ay, "Optimize one max problem by PSO and CSA," in *Lecture Notes in Networks and Systems*, vol. 693, Springer Nature Singapore, 2023, pp. 829–839, doi: 10.1007/978-981-99-3243-6_66.
- [17] W. A. Awadh, A. S. Alasady, and M. S. Hashim, "A multilayer model to enhance data security in cloud computing," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 32, no. 2, pp. 1105–1114, Nov. 2023, doi: 10.11591/ijeecs.v32.i2.pp1105-1114.
- [18] G. Yang, Y. Zhou, X. Chen, and C. Yu, "Fine-grained pseudo-code generation method via code feature extraction and transformer," in *Proceedings - Asia-Pacific Software Engineering Conference, APSEC*, IEEE, Dec. 2021, pp. 213–222, doi: 10.1109/APSEC53868.2021.00029.
- [19] K. Jang, A. Baksi, H. Kim, G. Song, H. Seo, and A. Chattopadhyay, "Quantum analysis of AES," *Cryptology ePrint Archive*, 2022, doi: 10.1007/978-981-97-0025-7_6.
- [20] S. A. Ajagbe, O. D. Adeniji, A. A. Olayiwola, and S. F. Abiona, "Advanced encryption standard (AES)-based text encryption for near field communication (NFC) using Huffman compression," *SN Computer Science*, vol. 5, no. 1, Jan. 2024, doi: 10.1007/s42979-023-02486-6.
- [21] Y. Ortakci and M. Y. Abdullah, "Performance analyses of AES and 3DES algorithms for encryption of satellite images," in *Lecture Notes in Networks and Systems*, vol. 183, Springer International Publishing, 2021, pp. 877–890, doi: 10.1007/978-3-030-66840-2_67.
- [22] N. Bhatia and S. Bhatia, "Changes in gender stereotypes over time: A computational analysis," *Psychology of Women Quarterly*, vol. 45, no. 1, pp. 106–125, Dec. 2021, doi: 10.1177/0361684320977178.
- [23] J. Wang and J. Li, "Blockchain and access control encryption-empowered IoT knowledge sharing for cloud-edge orchestrated personalized privacy-preserving federated learning," *Applied Sciences (Switzerland)*, vol. 14, no. 5, Feb. 2024, doi: 10.3390/app14051743.
- [24] S. M. Mohd *et al.*, "The performance of the 3DES and Fernet encryption in securing data files," *Journal of Theoretical and Applied Information Technology*, vol. 102, no. 3, pp. 812–820, 2024.
- [25] N. Yao *et al.*, "Efficient light coupling between an ultra-low loss lithium niobate waveguide and an adiabatically tapered single mode optical fiber," *Optics Express*, vol. 28, no. 8, Apr. 2020, doi: 10.1364/oe.391228.

BIOGRAPHIES OF AUTHORS



Osama Abd Qasim    received his M.Sc. degree in computer engineering technology in 2019 from Middle Technical University and B.E. in computer engineering technology in 2011 from Technical Engineering College of Mosul from Northern Technical University, working now as assist lecturer in Computer Engineering Technology Department, and he is also responsible for the systems and software division at the computer center-NTU. published one international paper in WSN for indoor localization. interested in computer engineering, computer communication, networks, MATLAB programs, IoT future world. He can be contacted at email: osama.hassani@ntu.edu.iq.



Sajjad Golshannavaz    was born in Urmia, Iran, in 1986. He received the B.Sc. (Honors) and M.Sc. (Honors) degrees in electrical engineering from Urmia University, Urmia, Iran, in 2009 and 2011, respectively. He received his Ph.D. degree in electrical power engineering from School of Electrical and Computer Engineering, University of Tehran, Tehran, Iran, in 2015. Currently, he is an associate professor in Electrical Engineering Department, Urmia University, Urmia, Iran. Since 2014 he has been collaborating with the Smart Electric Grid Research Laboratory, Department of Industrial Engineering, University of Salerno, Salerno, Italy. His research interests are in smart distribution grid operation and planning studies, design of distribution management system (DMS), demand side management (DSM) concepts and applications, microgrid design and operation studies, design of energy management system (EMS), application of FACTS controllers in power systems, application of intelligent controllers in power systems. He can be contacted at email: s.golshannavaz@urmia.ac.ir.