International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 10-No.4 (2024) pp. 1901-1906
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Performance and Security of AES, DES, and RSA in Hybrid Systems: An Empirical Analysis of Triple Encryption

Erman ÖZER[1]*, Hasan AYDOS[2]

[1]Recep Tayyip Erdoğan University, Faculty of Engineering and Architecture, Computer Engineering Department, Rize-Turkey
* **Corresponding Author Email:** erman.ozer@erdogan.edu.tr - **ORCID:** 0000-0002-9638-0233

[2]Recep Tayyip Erdoğan University, Faculty of Engineering and Architecture, Computer Engineering Department, Rize-Turkey
Email: hasan_aydos20@erdogan.edu.tr - **ORCID:** 0009-0008-1197-4093

Article Info:

DOI: 10.22399/ijcesen.694
Received : 27 November 2024
Accepted : 24 December 2024

Keywords :

Hybrid Encryption,
Cryptographic Algorithms,
Data Security,
Mamdani.

Abstract:

This study evaluates the performance and security of three cryptographic algorithms—AES, DES, and RSA—individually and in hybrid combinations. It aims to enhance information security through a novel three-step hybrid encryption method. Initially, each algorithm's execution time, memory usage, CPU usage, and data usage were analyzed separately. Subsequently, binary hybrid and triple hybrid techniques were assessed. The results indicate that AES is the fastest in terms of encryption speed, while RSA significantly increases memory usage in hybrid methods. DES exhibited the highest CPU usage. The triple hybrid method (AES + DES + RSA) demonstrated lower CPU and memory resource utilization, making it a viable option for applications requiring high security. This empirical analysis suggests that the triple hybrid method optimizes both performance and security, offering a balanced solution for secure data transmission. The findings contribute to the development of more effective data security methods and highlight the potential for further optimization and application in various contexts.

1. Introduction

As today's information technologies develop, the importance of information security is quite high. Recently, meetings, money transactions and all kinds of activities are carried out over the internet. This allows attackers to capture our private data and use our data in any way they want. Therefore, data privacy has become very important. For this reason, users want to keep their data secure while transmitting it and use these systems by ensuring data privacy

Individuals or organizations use cryptography encryption methods to prevent their information from being intercepted by other people or attackers while sharing information. With these recently used methods, users have aimed to prevent data leakage while ensuring data confidentiality. There are many symmetric and asymmetric algorithms to ensure information security.

Some of the symmetric algorithms are AES, DES, Blowfish and RC4. These algorithms ensure data integrity as well as data security. In any symmetric cryptographic algorithm, the same key is used to both encrypt and decrypt the file or data. This key is the only way to decrypt the encrypted data. This decrypts large amounts of data very quickly. One of the biggest problems with this is that access to the key is only securely kept between the sender and the receiver. These keys must be organized and kept secret, as anyone with the key can decrypt the data [1-4]. Unlike symmetric algorithms, asymmetric algorithms use two keys to encrypt and decrypt data: a public key and a private key.The public key is used to encrypt plaintext and the private key is used for decryption [5,6].Asymmetric algorithms ensure data security by relying entirely on prime number factorization. Asymmetric algorithms alone are not sufficient, even though they are considered undecipherable [7-11]. A few of the asymmetric algorithms are RSA, Diffie Helman and Merkle Helman. Even if precautions are taken with existing methods, attackers aim to capture this data. Existing studies have shown that

both symmetric and asymmetric algorithms can be used to decrypt, that is, existing encryptions can be broken.In this study, unlike the existing encryption methods, it is aimed to transmit the data to the other party with a 3-step encryption method without compromising the data integrity.AES, DES and RSA algorithms were first run and compared on their own. Then they were compared with binary hybrid techniques. Finally, the most secure 3-step hybrid method is discussed. The exec time, memory usage, cpu usage and data usage were analyzed. The second part of the study compares the work done in the literature, the third part provides information about the algorithms used and the dataset, the fourth part presents the results obtained and the last part contains the conclusion.

2. Literature Review

Abhishek et al. tried to find a solution by using RSA and DES encryption methods in a hybrid way in their system since the encryption systems used alone do not have enough solutions. They made a hybrid study according to the comparison of key management and key lengths in RSA and DES encryption methods[12]. While the advantage of the AES algorithm was used, the key management advantage of the RSA algorithm was used. Similarly, Vanaja et al. conducted a hybrid study to protect their system using AES and RSA methods. First of all, it was predicted that the RSA algorithm alone is disadvantageous when encrypting files, but it is more advantageous when AES and RSA algorithms are used together[13]. Sanap et al. compared different algorithms using data of different sizes. According to the results obtained, AES algorithm is more secure than other algorithms. Since Cipher-Block-Chaining (CBC) mode uses data blocks, it is more secure than Electronic Code Book (ECB) mode[14]. Saini et al. used different algorithms such as AES, RSA and MD5 for cloud security and compared their advantages and disadvantages in terms of memory size and time. They also used Enhanced Modern Symmetric Data Encryption (EMSDE) to protect data in the cloud environment. EMSDE is a symmetric encryption method that uses a single secret key to encrypt and decrypt data[15].

Meiyu et al. used Data Protection Application Programming Interface (DPAPI) algorithm and RSA algorithm in a hybrid way to authorize software in a more secure environment[16].

Sreehari emphasized the importance of key management in encryption algorithms. While he suggested sharing the key through a protected channel, he stated that he shared data securely by using Linear-feedback shift register (lfsr) key in his own work[17].When we look at the studies in encryption methods, secure and fast transmission of data is very important. As seen in most studies, algorithms are used either alone or as a binary hybrid. In this study, unlike other studies, AES, RSA and DES algorithms are used as a triple hybrid to provide the most secure transmission. The algorithms are compared in terms of processing time, memory used and CPU utilization in single, binary and triple.

3. Algorithms

3.1 Advanced Encryption Standard (AES)

AES was developed by the Belgian cryptographers Joan Daemen and Vincent Rijmen and standardized by NIST in 2001. It is a symmetric encryption method that protects important data in various areas such as communication networks, financial transactions and file storage. AES works with 128-bit data blocks and supports key sizes of 128, 192 or 256 bits, using substitutions, permutations and mixes to ensure encryption security. In symmetric encryption, the same key is used for both encryption and decryption, which requires secure key exchange between the parties. AES is widely used by governments, financial institutions and security-conscious companies, and is also used by the US National Security Agency (NSA) to protect top secret information. The algorithm applies a series of mathematical transformations to each 128-bit block of data, enabling efficient encryption on consumer devices and large-scale systems such as the IBM z14 mainframe series, which uses AES for blanket encryption. The security of AES increases exponentially with the key length, making a brute force attack impossible. Even with a 128-bit key, the computational effort required to crack AES exceeds the capabilities of the fastest supercomputers, making the method secure against current technological threats.

3.2 Data Encryption Standard(DES)

ES, a symmetric block cipher developed by an IBM team in the early 1970s and adopted by the National Institute of Standards and Technology (NIST), encrypts data in 64-bit blocks with a 56-bit key. Although the key length is technically 64 bits, only 56 bits are used for the encryption process. DES works with a 16-round Feistel structure and converts 64-bit plaintext blocks into ciphertext. As a symmetric key algorithm, DES uses the same key for both encryption and decryption. Despite its historical importance for data security, DES has become vulnerable to strong attacks, which has led to a decline in its use (figure 1).

CustomerId	Surname	CreditScore	Geography	Gender	Age	Tenure	NumOfProducts	Balance	HasCrCard	EstimatedSalary	Exited
3d01d26eab5ae407c5032b08e66f461d48847749d125b5119a	53f8aa7421f7e1	d9b9e6ad84dc239	c4f59ff8b7b1f83e93cd23	2b3e3993e6f25190	7d6c1eda9b2a3492ff21	aef1a867c40ecdd3	4325d79aa47a8cd34	198349150411cdd76ba2	228019b5e811fc379a87
6c102c4c26cf5f2585ffc2	0218e6a234b604e2	d9e6c1fee60c1a	56acd65068a6(	69c8d87b0866f5597	bf976ae11307e62a8ba(	f7d3513487a6c3d4	5c1f61f84c336c4e5bb6	d31330ab402ea3d(	f3acfbeea7ade77898	cd0ba4912dbbebe8bcf1f	f0dd2a28dce55ad9d9
596b22689cdf37c856684629ee7753fcd6ff0ec	7c5510a6f8e286	b6ec673f8436b	9b0b2b64db6ff34e	6935e31acb6b241b61d	07a313c5da73bfb43b327	d5dc093cec5dda	10ca766685e01d9f	3c09b4d52dae1e278	efae559307aee850060131	5968d4ae4f851651ec3
9a0ec9afb5960b2fbace	1f320d83251511e7f	b2262076dc456f	d998c5efdaf224	093fb4e7d59c6de3(	62946a20bd4f4844a1e	61cd220585b9ef91	a47fcb90a33dbd766b4	d347aa99c07c1ebf	674f65e4c816410fab	75897fdfea12e84f36e1	f9c29ec19a03eff407e43b
e2e80e723b26d307019e	b472d5d3cd199df9	dbfe6255481ba0	005570cf4104cc	dc182a241d79eee8	54c3ca88d1f3de55cf4f	17cf56c160ce94f8a	7f55b03187a68f6913e6	b2103b37a5e9e441	406d469117432bcf07	a52cb6d191ca7f202a156	508e9e8f7044b2c2162
c5e1a6cdecb329f23314	cae0d398e3ff0239b	ab73a4c34c879(	62b8ec4721cdc	631b249b963e05c1	756766156a865bcb5d5f	110b3460d08dd53(	929b80978b400ca0456	b05de3e06e4a3f39	8b9ea55222f2bcc84c5	1278ff0bfff3bd3f57883fa	f147d159e8a7610cc97(
f72c38ae87a6a071d405	e881959d6110e4af(	1ad439e570af61	46186c50af860(	35a9e83a0c4bea0(	dfae9344dca06123aaa	dc0de8c32077d51	91870f0c59df20c62226	e3297ce4f5580a2a	f7b4e8effada33321e(	918a5ab31b4ca5e0c12a(	2d00fb68c77fbb9f932
dad212b85fde943d02d6	1d8e3a4a7670890e	6f3616867 19baff	3d6f144c4fc35e	30cb23c6d48d19ee	1e267fda407f86602a7b	f01077f0f42e973a4	ea1e0f23cbd8873f23c8	cad9b4ed2589785(	97037fdad60c77ddd(	c4b78dfd4df31455b2861(	78329c1dc4366020ca:
bba9e59c026f55e258ab(	3dc4d9bd2b87157(	fd71975cf95705c	fd43f8a67858ff(	a3e4387d2a1f271a	3771cc3ffb6301033316(	ebfc336d4d3e8990	79dd1777562e74ad7f04(	dff8ed8d796941aa	b834ef2fc4289f6ba1(	d5fd914e4230175ff6b11f(	c95a81ddb197af242:
72115444fd892ec6dd4d2(	2cbccf668af4d0f4(	6ff206bcdbccdd	6eaf7c3f77e8ca	fac10fddb43c74da(	8ab2d244cf31740f086c(	f763394a696c73ca	7a25280bb992391cd09	0c4c5db23ec838f0	7d3b5b6020be38d20	fba2a57c048c03d121fb3(	ad3b169bbef2df9b41(
4bc4550d2f35f60a03486	39d441ee2aed574c	63b2bbb645db4	a80953ab79a1(	98355aeefb53a30d	a824ca5d66a00accd57	726878ef91faa7c9(	2053e19a41c012dc04b	990fd9e72e77f609e	b0fa16d990efb6ef21(	f93a574f93bfcfb7938d60(	7aebcc2d60af4f41086(
39a8591942e5380aad1e	fc0f1453c4b2d0fb9(	c32039dd2ccb3(	0b5ebe2741448	54bd7806e09346ef(	80001ca49e9b4801b6a(	6b3c964a4f2c18cd	eb133a637ffb63182600	55c0029f7bec14d5(	2656ef2e16814168e4	1f44a8b2d50d594bfed7(	f2c34c085fce4969ca9(
e8664d0461181e07067e(	e208d6cc4495783d	7601cdb989782f	21d5eec400752	229246b0d8b4ad718bbf	774c5f815c98b2d0	0fa556894bb146d0	dfe7d454be748f6a6896	f2462cbcd25b4923	013d55ab8f3dabd7e	96364936df4458ecbe5cfc	f4c25c7a3aa765fa7ca
9a0ec9afb5960b2fbace	1f320d83251511e7f	b2262076dc456f	d998c5efdaf224	093fb4e7d59c6de3(	62946a20bd4f4844a1e	61cd220585b9ef91	a47fcb90a33dbd766b4	d347aa99c07c1ebf	674f65e4c816410fab	75897fdfea12e84f36e1	f9c29ec19a03eff407e43

Figure 1. *Dataset*

CustomerId	Surname	CreditScore	Geography	Gender	Age	Tenure	Balance	NumOfProducts	HasCrCard	EstimatedSalary	Exited
15634602	Hargrave	619	France	Female	42	2	0	1	1	101348.88	1
15647311	Hill	608	Spain	Female	41	1	83807.86	1	0	112542.58	0
15619304	Onio	502	France	Female	42	8	159660.8	3	1	113931.57	1
15701354	Boni	699	France	Female	39	1	0	2	0	93826.63	0
15737888	Mitchell	850	Spain	Female	43	2	125510.82	1		79084.1	0
15574012	Chu	645	Spain	Male	44	8	113755.78	2	1	149756.71	1
15592531	Bartlett	822	France	Male	50	7	0	2	1	10062.8	0
15656148	Obinna	376	Germany	Female	29	4	115046.74	4	1	119346.88	1
15767821	Bearce	528	France	Male	31	6	102016.72	2	0	80181.12	0
15737173	Andrews	497	Spain	Male	24	3	0	2	1	76390.01	0
15632264	Kay	476	France	Female	34	10	0	2	1	26260.98	0
15691483	Chin	549	France	Female	25	5	0	2	0	190857.79	0
15600882	Scott	635	Spain	Female	35	7	0	2	1	65951.65	0
15643966	Goforth	616	Germany	Male	45	3	143129.41	2	0	64327.26	0

Figure 2. *Encrypted data with in the dataset*

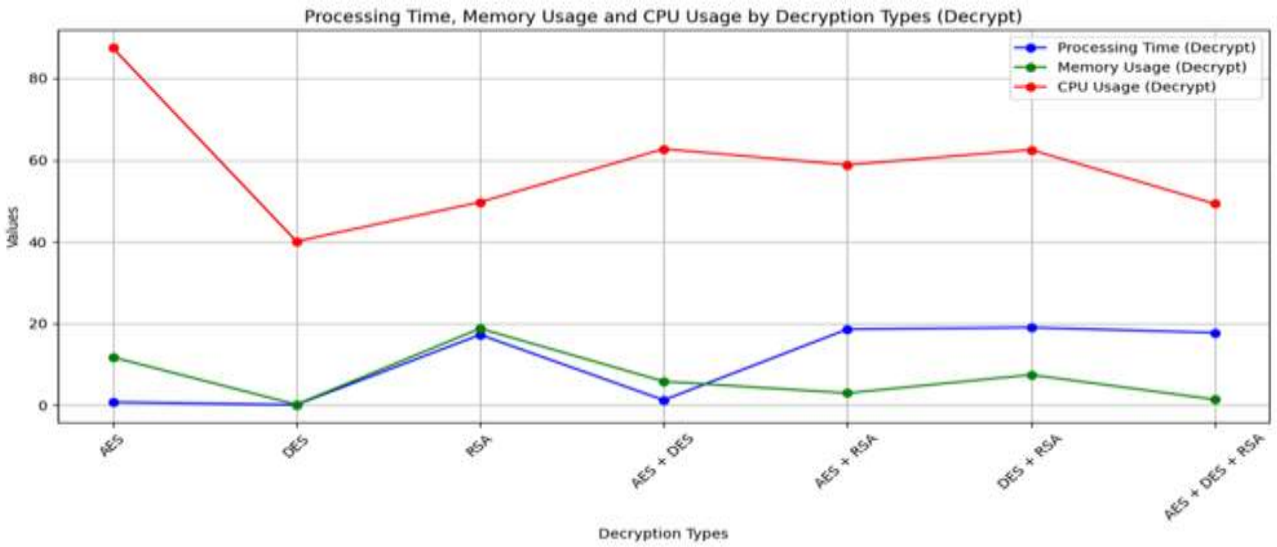

Figure 3. *Encrypt results*

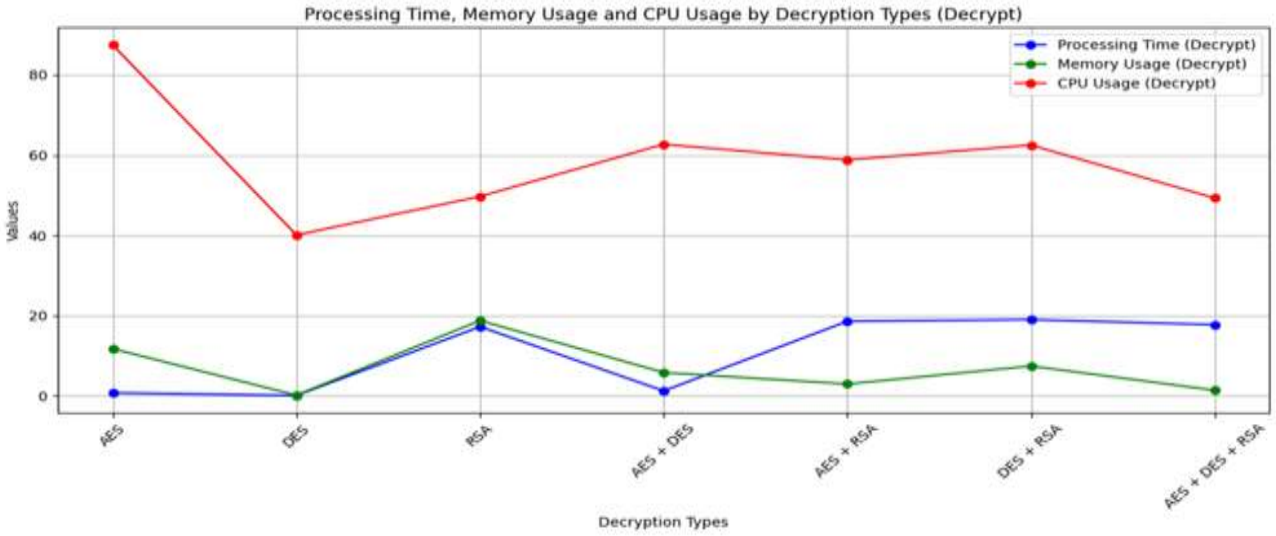

Figure 4. *Decrypt results*

3.3 Rivest-Shamir-Adleman (RSA)

RSA, an asymmetric encryption algorithm named after its developers Rivest, Shamir and Adleman, was first described at MIT in 1977. This algorithm is based on the principle of Public Key Cryptography (PKC), in which a publicly known key is used for encryption and another, private key for decryption. The public key is generated by multiplying two large prime numbers that result in a product of 1024, 2048 or 4096 bits, while decryption requires knowledge of these prime factors. RSA is more computationally intensive and slower than AES and is typically used for encryption of small amounts of data, digital signatures and key exchange. Its slower performance and higher complexity make it unsuitable for encrypting large amounts of data.

4. Dataset

The dataset consists of 10000 rows. It consists of 12 attributes: CustomerId, Surname, CreditScore, Geography(France, Spain or Germany), Gender, Age, Tenure(The number of years the customer has been with the bank), Balance(The customer's account balance), NumOfProducts(The number of bank products the customer uses), HasCrCard (Whether the customer has a credit card) , EstimatedSalary, Exited(Whether the customer has churned).

5. Results and Analysis

Figure 2 shows the encrypted version of the hybrid system. Figure 3 is encrypt results and also figure 4 shows decrypt results.

In this study, the performances of AES, DES, and RSA algorithms were compared individually, in dual hybrid, and triple hybrid methods to ensure data security. Based on encryption and decryption results, AES was observed to be the fastest among the three algorithms in terms of encryption speed. Regarding memory usage, AES and DES maintained similar levels, whereas RSA consumed more memory. These findings suggest that the use of RSA encryption in hybrid encryptions significantly increases memory usage. Another metric used for comparison was CPU usage, which was highest for DES. The lowest CPU usage was observed in the triple encryption technique, AES + DES + RSA hybrid encryption. During decryption, similar to encryption comparisons, AES was observed to be faster than the others. In terms of memory usage during decryption, AES and DES maintained similar levels as in encryption, while the RSA encryption algorithm continued to require more memory. These results indicate that the RSA encryption algorithm significantly increases memory usage in hybrid encryptions. Another comparative metric showed that CPU usage during decryption was highest for AES, while DES exhibited the lowest CPU usage. When considering the triple hybrid encryption, which offers the highest security, it ranked second in overall metric comparisons. According to these findings, the triple hybrid method provides more secure data transmission while also utilizing lower CPU and memory resources.

These findings suggest that the triple hybrid method can be employed in applications requiring high security and offers more optimal results in cost and performance evaluations compared to other encryption techniques.

In the future, further optimization and testing in different application contexts could expand the potential application areas of these methods.

6. Conclusion

This study provides a comprehensive evaluation of AES, DES, and RSA cryptographic algorithms, both individually and in hybrid combinations, to enhance data security through a three-step hybrid encryption method. The empirical analysis reveals that AES is the most efficient in terms of encryption speed, while RSA, despite its robust security, significantly increases memory usage in hybrid systems. DES, on the other hand, exhibits the highest CPU usage. The triple hybrid method (AES + DES + RSA) demonstrated superior performance by balancing security with lower CPU and memory resource utilization, making it a viable option for applications requiring stringent data security. The findings suggest that the triple hybrid method optimizes both security and performance, offering a cost-effective solution for secure data transmission. Future research could focus on further optimization and testing in diverse application contexts to expand the potential applicability of these methods. This study's contributions are pivotal for developing new and effective data security strategies, ensuring robust protection against evolving cyber threats. Data Security is important and studied in literature widely and reported [18-29].

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **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
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] S. Kumar, M. S. Gaur, P. Sagar Sharma and D. Munjal, (2021). A Novel Approach of Symmetric Key Cryptography, *2nd International Conference on Intelligent Engineering and Management (ICIEM)*, 2021, pp. 593-598, doi: 10.1109/ICIEM51511.2021.9445343.

[2] A. Markandey, P. Dhamdhere and Y. Gajmal, (2018) "Data Access Security in Cloud Computing: A Review," 2018 *International Conference on Computing, Power and Communication Technologies (GUCON)*, Greater Noida, Uttar Pradesh, India, 2018, pp. 633-636.doi: 10.1109/GUCON.2018.8675033

[3] A. Kumar, V. Jain and A. Yadav, (2020). A New Approach for Security in Cloud Data Storage for IOT Applications Using Hybrid Cryptography Technique," 2020 *International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC)*, Mathura, Uttar Pradesh, India, 2020, pp. 514-517, doi: 10.1109/PARC49193.2020.236666

[4] Dahiya, O. and Solanki, K. (2019). Comprehensive Cognizance of Regression Test Case Prioritization Techniques, *International Journal of Emerging Trends in Engineering Research*, 7(11);638-646. DOI: 10.30534/ijeter/2019/377112019

[5] P. Gupta, D. Kumar Verma and A. Kumar Singh, (2018). Improving RSA Algorithm Using Multi-Threading Model for Outsourced Data Security in Cloud Storage," 2018 *8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida*, 2018, pp. 14-15.doi: 10.1109/CONFLUENCE.2018.8442788

[6] D. M. Alsaffar et al., (2020). Image Encryption Based on AES and RSA Algorithms," 2020 *3rd International Conference on Computer Applications & Information Security (ICCAIS)*, Riyadh, Saudi Arabia, 2020, pp. 1-5, doi: 10.1109/ICCAIS48893.2020.9096809

[7] S. Kumar, M. S. Gaur, P. Sagar Sharma and D. Munjal, (2021). A Novel Approach of Symmetric Key Cryptography, 2021 *2nd International Conference on Intelligent Engineering and Management (ICIEM)*, 2021, pp. 593-598, doi: 10.1109/ICIEM51511.2021.9445343

[8] G. Jain and V. Sejwar, (2017). Improving the security by using various cryptographic techniques in cloud computing, 2017 *International Conference on Intelligent Computing and Control Systems (ICICCS)*, *Madurai*, pp. 23-28.doi: 10.1109/ICCONS.2017.8250721

[9] S. A. Ahmad and A. B. Garko, (2019). Hybrid Cryptography Algorithms in Cloud Computing: A Review," 2019 *15th International Conference on Electronics, Computer and Computation (ICECCO)*, Abuja, Nigeria, 2019, pp. 1-6, doi: 10.1109/ICECCO48375.2019.9043254.

[10] Sanap, S. D., & More, V. (2021). Analysis of Encryption Techniques for Secure Communication. 2021 *International Conference on Emerging Smart Computing and Informatics* (ESCI). doi:10.1109/esci50559.2021.9396926.

[11] E. Özer and H. Aydos, "Utilizing Hybrid Encryption Methods to Ensure the Security of Financial

Transactions," 2024 8th *International Artificial Intelligence and Data Processing Symposium (IDAP), Malatya, Turkiye, 2024*, pp. 1-4, doi: 10.1109/IDAP64064.2024.10710781.

[12] Guru, M.A., & Ambhaikar, A. (2021). AES and RSA-based Hybrid Algorithms for Message Encryption & Decryption. *Information Technology in Industry*, 9(1), 273-279. doi:10.17762/itii.v9i1.129.

[13] V. Malgari, R. Dugyala and A. Kumar, (2019). A Novel Data Security Framework in Distributed Cloud Computing, 2019 *Fifth International Conference on Image Information Processing* (ICIIP), Shimla, India, 2019, pp. 373-378, doi: 10.1109/ICIIP47207.2019.8985941.

[14] Sanap, S. D., & More, V. (2021). Analysis of Encryption Techniques for Secure Communication. 2021 *International Conference on Emerging Smart Computing and Informatics* (ESCI). doi:10.1109/esci50559.2021.9396926

[15] K. Saini, V. Agarwal, A. Varshney and A. Gupta, (2018).E2EE For Data Security For Hybrid Cloud Services: A Novel Approach, *2018 International Conference on Advances in Computing, Communication Control and Networking* (ICACCCN), Greater Noida (UP), India, 2018, pp. 340-347. doi: 10.1109/ICACCCN.2018.8748782

[16] Jin Meiyu, Tang Yaling, Zhang Xuefeng (2020). Hybrid encryption algorithm of DPAPI and RSA [J]. *Computer System Application*, 29 (11): 151-156. doi: 10.15888/j.cnki.CsA.007673.

[17] K. N. Sreehari, (2018). Efficient key management methods for symmetric cryptographic algorithm", in 2018 *IEEE International Conference on Computational Intelligence and Computing Research* (ICCIC).

[18] R, U. M., P, R. S., Gokul Chandrasekaran, & K, M. (2024). Assessment of Cybersecurity Risks in Digital Twin Deployments in Smart Cities. *International Journal of Computational and Experimental Science and Engineering*, 10(4);695-700. https://doi.org/10.22399/ijcesen.494

[19] Prasada, P., & Prasad, D. S. (2024). Blockchain-Enhanced Machine Learning for Robust Detection of APT Injection Attacks in the Cyber-Physical Systems. *International Journal of Computational and Experimental Science and Engineering*, 10(4);799-810. https://doi.org/10.22399/ijcesen.539

[20] Srinivas Aluvala, & V. Srikanth. (2024). Characterization of Destructive Nodes and Analysing their Impact in Wireless Networks. *International Journal of Computational and Experimental Science and Engineering*, 10(4);1584-1593. https://doi.org/10.22399/ijcesen.726

[21] S, P., & A, P. (2024). Secured Fog-Body-Torrent : A Hybrid Symmetric Cryptography with Multi-layer Feed Forward Networks Tuned Chaotic Maps for Physiological Data Transmission in Fog-BAN Environment. *International Journal of Computational and Experimental Science and Engineering*, 10(4);671-681. https://doi.org/10.22399/ijcesen.490

[22] MOHAMED, N. N., Yulianta SIREGAR, Nur Arzilawati MD YUNUS, & Fazlina MOHD ALI. (2024). Modelling the Hybrid Security Approach for Secure Data Exchange: A Proof of Concept . *International Journal of Computational and Experimental Science and Engineering*, 10(4);1475-1485. https://doi.org/10.22399/ijcesen.344

[23] M. Swetha, & G. Appa Rao. (2024). Hybrid Ensemble Lightweight Cryptosystem for Internet of Medical Things Security. *International Journal of Computational and Experimental Science and Engineering*, 10(4);1528-1540. https://doi.org/10.22399/ijcesen.625

[24] Kosaraju Chaitanya, & Gnanasekaran Dhanabalan. (2024). Precise Node Authentication using Dynamic Session Key Set and Node Pattern Analysis for Malicious Node Detection in Wireless Sensor Networks. *International Journal of Computational and Experimental Science and Engineering*, 10(4);1462-1474. https://doi.org/10.22399/ijcesen.613

[25] B. Jayakumar, & S. Prabakar. (2024). A Case study on MGNREGA and social security in Tamil Nadu's Krishnagiri district, India. *International Journal of Computational and Experimental Science and Engineering*, 10(4);1290-1299. https://doi.org/10.22399/ijcesen.712

[26] El-Taj, H. (2024). A Secure Fusion: Elliptic Curve Encryption Integrated with LSB Steganography for Hidden Communication. *International Journal of Computational and Experimental Science and Engineering*, 10(3);434-460. https://doi.org/10.22399/ijcesen.382

[27] Suneetha Madduluri, & T. Kishorekumar. (2024). Multimodal Biometric Authentication System for Military Weapon Access: Face and ECG Authentication. *International Journal of Computational and Experimental Science and Engineering*, 10(4);952-961. https://doi.org/10.22399/ijcesen.565

[28] G. Saraniya, & C. Yamini. (2024). Design of Effective Amplification Signal by Controlling Bandwidth Using Adaptive Learning Technique In Voice Over Internet Protocol. *International Journal of Computational and Experimental Science and Engineering*, 10(4);1661-1672. https://doi.org/10.22399/ijcesen.659

[29] Godavarthi, S., & G., D. V. R. (2024). Federated Learning's Dynamic Defense Against Byzantine Attacks: Integrating SIFT-Wavelet and Differential Privacy for Byzantine Grade Levels Detection. *International Journal of Computational and Experimental Science and Engineering*, 10(4);775-786. https://doi.org/10.22399/ijcesen.538