EasyChair Preprint

№ 13536

Fortifying Information Security: a Comparative Analysis of AES, DES, 3DES, RSA, and Blowfish Algorithm

Muhammad Rameel and Zain Asif

June 3, 2024

Fortifying Information Security: A Comparative Analysis of AES, DES, 3DES, RSA, and Blowfish Algorithm

Muhammad Rameel
Department of Computer Science
Sir Syed College of Computer Science
Affiliated with University of
Engineering and Technology Lahore
Lahore, Pakistan
rameelkamboh@gmail.com

Zain Asif
Department of Computer Science
Sir Syed College of Computer Science
Affiliated with University of
Engineering and Technology Lahore
Lahore, Pakistan
zainasif571@gmail.com

***Abstract*: In the ever-evolving landscape of information security, selecting the most suitable encryption algorithm is crucial. This paper presents a comparative analysis of five prominent encryption algorithms: Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES (3DES), Rivest-Shamir-Adleman (RSA), and Blowfish. Through an in-depth exploration of each algorithm's cryptographic principles and practical implementations, this study evaluates their efficacy in fortifying information security across various metrics. The analysis encompasses ciphering and deciphering timeframes, memory overhead, tunability, throughput, algorithmic complexity, scalability, and security strengths. AES is highly regarded for its strength and adaptability, making it widely used. DES, though historically important, is now weak due to its short key size, with 3DES improving security by extending key lengths. RSA is essential for secure communication but has performance issues. Blowfish is simple, resistant to brute-force attacks, and offers variable key lengths. By scrutinizing these algorithms across multiple dimensions, this comparative analysis aims to provide insights into selecting the most appropriate encryption method to fortify information security in various contexts.**

Keywords: Information Security, AES (Advanced Encryption Standard), DES (Data Encryption Standard), 3DES (Triple Data Encryption Standard), RSA (Rivest-Shamir-Adleman), Blowfish Algorithm.

I. INTRODUCTION

Encryption is crucial for protecting sensitive information, such as health and banking data, from unauthorized access and exploitation. The vulnerability of such data highlights the need for robust encryption algorithms to ensure privacy and confidentiality [1]. In sectors like banking, healthcare, and the military, where data breaches can have severe consequences, encryption is fundamental for safeguarding data integrity and user privacy [5]. The adoption of encryption algorithms is essential for securing information transmission and preventing unauthorized disclosure of confidential data [4]. By leveraging these algorithms, organizations can mitigate risks associated with data breaches and unauthorized access, thereby maintaining stakeholder trust [8]. Researchers and practitioners have consistently turned to encryption algorithms to strengthen information security across various domains, including financial transactions and military communications [2][5].

Understanding encryption's effectiveness requires familiarity with key cryptographic algorithms that underpin modern security protocols. This section introduces five prominent encryption algorithms: Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES (3DES), Rivest-Shamir-Adleman (RSA), and Blowfish. Each algorithm has distinct cryptographic principles and operational characteristics, providing a versatile set of encryption techniques tailored to specific security needs. By exploring these algorithms, readers gain insights into their strengths, limitations, and practical applications in enhancing information security [3][7]. AES is known for its robustness, versatility, and widespread adoption. Developed to address the limitations of DES, AES offers a flexible framework for secure data transmission across various domains. Its scalability, efficient encryption and decryption processes, and resistance to cryptanalytic attacks make it a cornerstone of contemporary encryption standards [9][12]. DES, a seminal encryption algorithm from the 1970s, retains historical significance despite its limited key size and susceptibility to brute-force attacks. While its adoption has declined with the emergence of more robust standards like AES, DES's foundational role in shaping cryptographic principles remains significant [11].

3DES enhances DES by using multiple encryption rounds, providing higher security for applications needing backward compatibility. Despite its slower processing compared to newer methods, 3DES is still viable for certain security contexts due to its resilience against brute-force attacks and reliability in various Internet protocols [16]. RSA introduced asymmetric encryption, enabling secure communication and digital signatures. By generating distinct public and private keys, RSA ensures data confidentiality and integrity, despite performance impacts due to its reliance on large prime numbers. RSA's widespread adoption underscores its importance in modern cryptographic protocols [5][4]. Blowfish, introduced in the early 1990s, combines simplicity, efficiency, and security, making it a preferred choice for securing sensitive data. Its variable key lengths and resistance to brute-force attacks provide a versatile encryption solution for diverse applications, ranging from software to hardware implementations. Its open-source nature and compatibility with different key lengths further enhance its appeal in the cybersecurity landscape [1][10].

This comparative analysis aims to provide comprehensive insights into the strengths, weaknesses, and practical implications of these prominent encryption algorithms. By examining factors such as encryption and decryption speed, memory overhead, scalability, and security, this study helps

decision-makers select the most suitable encryption method for enhancing information security in various contexts [20]. Through an evidence-based approach, readers gain a nuanced understanding of the trade-offs inherent in different encryption algorithms, enabling informed decisions in implementing robust encryption strategies [23].

II. Encryption Fundamentals

A. Basic Principles of Encryption

Encryption relies on confidentiality and integrity. Confidentiality ensures that only authorized parties can access the data using cryptographic keys, while integrity ensures the data remains unaltered during transmission and storage [13][9].

B. Components and Techniques

Encryption algorithms include key generation mechanisms, substitution-permutation operations, key expansion functions, and iterative encryption schemes. Symmetric encryption uses a single key for both encryption and decryption, while asymmetric encryption uses a pair of public and private keys. Hybrid and quantum encryption methods offer enhanced security [22][10][14][4][19].

C. Evolution of Encryption Technology

Encryption technology has advanced from simple ciphers to complex algorithms like AES and RSA, designed to resist sophisticated attacks [6][5].

D. Importance in Information Security

Encryption protects sensitive data from unauthorized access and interception, mitigating risks of data breaches and ensuring compliance with regulatory requirements [4].

III. Understanding AES, DES, 3DES, RSA, and Blowfish: An Overview

A. Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a symmetric key encryption algorithm developed by Vincent Rijmen and Joan Daemen in 1998 and adopted as a standard by the National Institute of Standards and Technology (NIST) in 2001. AES was designed to replace the Data Encryption Standard (DES) due to its enhanced security features and efficiency. It operates on fixed-size blocks of data (128 bits) and supports key sizes of 128, 192, and 256 bits. The algorithm's structure is based on a substitution-permutation network (SPN) that includes multiple rounds of processing to transform plaintext into cipher text. Each round consists of several steps: Sub Bytes (substitution of bytes using a substitution table), Shift Rows (cyclically shifting rows of the state array), Mix Columns (mixing the columns of the state array using matrix multiplication), and Add Round Key (combining the state with a portion of the key using the XOR operation). The number of rounds depends on the key length: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys [1].

AES is highly regarded for its security and performance. The SPN structure ensures a high level of diffusion and confusion, making it resistant to various forms of cryptanalytic attacks such as differential and linear cryptanalysis. Additionally, AES incorporates a key expansion algorithm that generates a series of round keys from the initial key, ensuring that each round has a unique key for processing. The efficiency of AES is notable in both hardware and software implementations, making it suitable for a wide range of applications, including secure communications, financial transactions, and data storage. Its adoption in protocols such as SSL/TLS, IPsec, and WPA2 underscores its importance in securing internet and wireless communications [12].

Despite its robust security features, AES continues to be the subject of ongoing research and scrutiny to ensure its resilience against emerging threats. Researchers are exploring techniques to enhance AES's resistance to side-channel attacks, such as differential power analysis and fault injection attacks, which exploit physical implementations of the algorithm. Furthermore, with the advent of quantum computing, there is an ongoing effort to evaluate the impact of quantum algorithms on AES's security and to develop post-quantum cryptographic algorithms that can provide security in the era of quantum computing. AES's adaptability and continuous improvement efforts ensure its relevance and reliability in the evolving landscape of cryptography [5].

B. Data Encryption Standard (DES) and Triple DES (3DES)

The Data Encryption Standard (DES) was developed by IBM in the early 1970s and became a widely adopted encryption standard after being endorsed by the National Institute of Standards and Technology (NIST) in 1977. DES is a symmetric key block cipher that encrypts data in 64-bit blocks using a 56-bit key through 16 rounds of permutation, substitution, and XOR operations. Each round of DES includes a series of complex transformations designed to obscure the relationship between the plaintext and the cipher text, thereby providing security against various types of cryptanalytic attacks. However, over time, the key length of 56 bits proved to be insufficient in the face of increasing computational power, making DES vulnerable to brute-force attacks, where attackers attempt all possible keys until the correct one is found [1].

To address the security limitations of DES, Triple DES (3DES) was introduced. 3DES enhances the original DES algorithm by applying the DES encryption process three times in succession with either two or three distinct keys. This effectively extends the key length to 112 or 168 bits, significantly increasing the complexity of brute-force attacks. The encryption process in 3DES typically involves an encrypt-decrypt-encrypt (EDE) sequence, where the data is first encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key. This layered approach ensures that even if an attacker manages to compromise one of the keys, the data remains secure due to the additional encryption layers [5].

Despite the improved security provided by 3DES, it has some drawbacks, including slower processing speeds compared to more modern encryption algorithms like AES. The increased computational requirements of applying the DES algorithm three times can impact performance,

especially in high-speed network environments or resource-constrained devices. As a result, 3DES is being gradually phased out in favor of more efficient and secure encryption standards. Nevertheless, 3DES remains in use in certain legacy systems and specific applications where backward compatibility with DES is necessary. The continued use of 3DES highlights the importance of maintaining a balance between security and performance while transitioning to newer cryptographic technologies [17][6].

C. RSA Encryption

The RSA algorithm, named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, is a fundamental public key cryptosystem introduced in 1977. RSA revolutionized cryptography by providing a method for secure communication over untrusted networks using asymmetric encryption. Unlike symmetric encryption algorithms, which use the same key for both encryption and decryption, RSA uses a pair of keys: a public key for encryption and a private key for decryption. The security of RSA is based on the computational difficulty of factoring large composite numbers, a problem for which no efficient solution currently exists. The key generation process involves selecting two large prime numbers, multiplying them to obtain a modulus, and then deriving the public and private keys from this modulus [15][1].

RSA's versatility extends beyond encryption to include digital signatures, which provide authentication and integrity for digital messages. In a digital signature scheme, the sender uses their private key to generate a signature on the message, and the recipient uses the sender's public key to verify the signature. This process ensures that the message has not been tampered with and that it originated from the purported sender. The widespread adoption of RSA in various security protocols, such as SSL/TLS for secure web browsing, PGP for secure email communication, and digital certificates for identity verification, underscores its critical role in ensuring the security of digital communications [19].

Despite its strengths, RSA has some limitations, primarily related to performance and key management. The encryption and decryption processes in RSA are computationally intensive, especially when using large key sizes required for strong security. Key lengths of 2048 bits or more are commonly used to ensure security against current computational capabilities, but these longer keys can result in slower encryption and decryption operations. Additionally, RSA's security depends on the secure generation and storage of keys, as the compromise of the private key would render the encryption ineffective. To address these challenges, hybrid encryption schemes often combine RSA with symmetric encryption algorithms, using RSA to securely exchange a symmetric key, which is then used for efficient bulk encryption. This approach leverages the strengths of both types of cryptography to achieve a balance between security and performance[18].

D. Blowfish Algorithm

Blowfish is a symmetric key block cipher designed by Bruce Schneier in 1993 as a fast and secure alternative to existing encryption algorithms at the time, such as DES. It encrypts data in 64-bit blocks and supports variable key lengths ranging from 32 bits to 448 bits, making it flexible and adaptable to various security needs. The design of Blowfish emphasizes simplicity and efficiency, making it suitable for applications where performance is a critical consideration. The algorithm consists of two main parts: the key-expansion and the data-encryption phases. During key expansion, the original key is transformed into several sub keys totaling 4168 bytes. These sub keys are used in the data encryption phase, which consists of 16 rounds of processing involving permutation and substitution [1][13].

Blowfish's architecture is designed to be both fast and secure. Each round of the encryption process involves complex operations, including key-dependent S-boxes and bitwise exclusive-or (XOR) operations. The S-boxes are initialized using the key and undergo several iterations of encryption to ensure that each bit of the key influences many parts of the algorithm, a principle known as the avalanche effect. This ensures that even small changes in the plaintext or key result in significantly different cipher text, enhancing the security of the encrypted data. The efficient design of Blowfish makes it particularly suitable for implementation in both software and hardware, where high throughput and low latency are important [14].

Despite its strengths, Blowfish has some limitations and challenges. One of the main concerns is its 64-bit block size, which is considered insufficient for modern encryption standards. With the increase in computational power and the amount of data being processed, the risk of birthday attacks, where duplicate blocks of cipher text can reveal patterns, becomes more significant. Additionally, the complexity of the key schedule has led to some vulnerabilities in certain implementations, particularly those that do not use sufficiently random keys or fail to implement the key schedule correctly. As a result, while Blowfish remains a secure and efficient option for many applications, its use has declined in favor of newer algorithms like AES, which offer larger block sizes and are more resistant to modern cryptographic attacks [22].

Blowfish's legacy in the field of cryptography is notable, as it paved the way for more advanced and secure encryption algorithms. It served as a foundation for the development of the Twofish algorithm, also designed by Bruce Schneier, which was a finalist in the competition to select the Advanced Encryption Standard (AES). Twofish incorporates many of the principles of Blowfish but addresses its limitations, such as the block size and key schedule complexities. Today, Blowfish is still used in some applications, particularly in secure storage systems and network protocols where its efficiency and flexibility are advantageous. However, for most new applications, AES has become the preferred choice due to its superior security and broader acceptance in industry standards[1][23].

IV. COMPARATIVE ANALYSIS METHODOLOGY

A. Ciphering Timeframe

- AES: Generally fast ciphering timeframe due to its efficient block cipher structure and optimized implementations.

- DES: Relatively slower compared to AES due to its simpler structure and smaller key size, which can lead to faster brute-force attacks.
- 3DES: Slower than AES due to its triple encryption process, which involves performing the DES algorithm three times.
- RSA: Slower ciphering timeframe compared to symmetric key algorithms like AES and DES due to its asymmetric encryption process and complex mathematical operations.
- Blowfish: Generally fast ciphering timeframe due to its efficient structure and variable key lengths, providing flexibility without compromising speed.

B. *Deciphering Timeframe*

- AES: Deciphering is generally fast, mirroring the ciphering timeframe.
- DES: Deciphering is slower compared to AES due to its simpler structure and smaller key size, similar to the ciphering process.
- 3DES: Deciphering is slower than AES due to the triple encryption process, but it remains a viable option for backward compatibility.
- RSA: Deciphering is slower compared to symmetric key algorithms due to its asymmetric nature and reliance on complex mathematical operations.
- Blowfish: Deciphering is generally fast, reflecting the efficient encryption process of the algorithm.

C. *Memory Overhead*

- AES: Requires moderate memory overhead, depending on implementation and key size.
- DES: Generally low memory overhead due to its simpler structure and smaller key size.
- 3DES: Higher memory overhead compared to AES and DES due to the triple encryption process, especially when using three distinct keys.
- RSA: Higher memory overhead compared to symmetric key algorithms due to the storage requirements for public and private keys.
- Blowfish: Requires moderate memory overhead, depending on the key size and implementation.

D. *Tunability*

- AES: Offers tunability through key length selection, providing flexibility in balancing security and performance.
- DES: Limited tunability due to fixed block size and key length.
- 3DES: Limited tunability compared to AES due to the fixed block size and reliance on multiple encryption rounds.
- RSA: Offers tunability through key size selection, allowing users to adjust security levels.
- Blowfish: Highly tunable with variable key lengths, providing flexibility in balancing speed and security.

E. *Throughput Comparison*

- AES: Generally offers high throughput due to its efficient structure and widespread hardware and software optimizations.
- DES: Lower throughput compared to AES due to its simpler structure and smaller key size.
- 3DES: Lower throughput compared to AES due to the triple encryption process.
- RSA: Lower throughput compared to symmetric key algorithms due to its asymmetric nature and reliance on complex mathematical operations.
- Blowfish: Generally offers high throughput due to its efficient structure and variable key lengths.

F. *Scalability*

- AES: Highly scalable due to its efficient structure and support for different key lengths, suitable for various security requirements.
- DES: Limited scalability due to fixed block size and key length.
- 3DES: Limited scalability compared to AES due to slower performance and reliance on triple encryption process.
- RSA: Moderately scalable, with key size adjustments to accommodate evolving security needs.
- Blowfish: Moderately scalable with variable key lengths, providing flexibility in adapting to different security levels.

G. *Security Strengths*

- AES: Strong security with resistance against various cryptographic attacks, widely adopted as a standard encryption algorithm.
- DES: Weaker security compared to modern standards like AES, vulnerable to brute-force attacks due to its small key size.
- 3DES: Offers stronger security compared to DES, but slower performance and being phased out in favor of AES.
- RSA: Strong security based on the difficulty of integer factorization, widely used for secure communication and digital signatures.
- Blowfish: Strong security with resistance against brute-force attacks, offering a reliable encryption solution for various applications.

H. *Algorithmic Complexity Examination*

- AES: Complex algorithm with sophisticated mathematical operations, resistant to cryptanalytic attacks.
- DES: Relatively simple algorithm with known vulnerabilities, susceptible to brute-force attacks.
- 3DES: Complex algorithm due to triple encryption process, providing enhanced security compared to DES but slower performance.

- RSA: Complex algorithm relying on number theory, with security based on the difficulty of integer factorization.
- Blowfish: Moderately complex algorithm with efficient substitution and permutation operations, offering robust security.

TABLE I.

Criteria	*AES*	*DES*	*3DES*	*RSA*	*Blowfish*
Ciphering Time frame	Fast	Slow	Slow	Moderate to Slow	Fast
Deciphering Time frame	Fast	Slow	Slow	Moderate to Slow	Fast
Memory Overhead	Low to Moderate	Low to Moderate	Moderate to High	Low to Moderate	Low to Moderate
Tunability	High	Low	Low	Moderate	High
Throughput	High	Low	Low	Moderate	High
Algorithmic Complexity	High	Low	Moderate	High	Moderate
Scalability	High	Low	Low	Moderate	High
Security Strengths	High	Low	Moderate	High	High

Fig. 1. Comparitive Analysis.

Figure Labels: Based on this analysis, AES emerges as a robust and versatile encryption algorithm, offering strong security, high throughput, and scalability. However, the choice of algorithm depends on specific requirements such as speed, security level, and compatibility.

V. CONCLUSION

Firstly, in terms of ciphering and deciphering timeframes, AES demonstrates superiority with generally fast processing due to its efficient block cipher structure and widespread hardware and software optimizations. Conversely, DES and 3DES exhibit slower performance, particularly 3DES due to its triple encryption process, making them less favorable options for applications where speed is paramount. RSA, being asymmetric, naturally lags in processing speed compared to symmetric key algorithms like AES and DES. Blowfish, however, stands out for its generally fast ciphering and deciphering timeframes, attributed to its efficient structure and variable key lengths. Memory overhead considerations reveal moderate requirements for AES and Blowfish, while DES and RSA tend towards lower to moderate overhead due to their simpler structures. 3DES, however, demonstrates higher memory overhead, especially when utilizing three distinct keys. Tunability, a crucial aspect for tailoring security levels to specific requirements, is notably strong in AES and Blowfish, offering flexibility through key length adjustments. DES and 3DES, constrained by fixed block sizes and key lengths, exhibit limited tunability in comparison. RSA falls within a moderate range of tunability, with adjustments made to key sizes. Throughput comparisons emphasize AES's dominance in offering high throughput, owing to its efficient structure and widespread optimizations. Conversely, DES and 3DES exhibit lower throughput due to their slower processing, with RSA similarly lagging behind due to its asymmetric nature. Blowfish, however, aligns closely with AES in providing high throughput, attributed to its efficient structure and variable key lengths. Algorithmic complexity analysis underscores AES's robust security, supported by sophisticated mathematical operations and resistance against various cryptographic attacks. DES, although simpler, suffers from known vulnerabilities, making it less secure compared to modern standards like AES. 3DES offers enhanced security over DES but at the expense of slower performance. RSA's security strengths lie in its reliance on the difficulty of integer factorization, making it a widely used choice for secure communication and digital signatures. Blowfish demonstrates strong security, particularly against brute-force attacks, offering a reliable encryption solution for diverse applications. In conclusion, while each encryption algorithm exhibits strengths and weaknesses across various criteria, AES emerges as the most robust and versatile option, balancing strong security, high throughput, scalability, and tunability. DES and 3DES, while still utilized in certain legacy systems, are generally surpassed by AES in terms of security and performance. RSA remains a viable choice for asymmetric encryption needs, particularly in key exchange and digital signatures, albeit with slower processing. Blowfish, while offering strong security and efficiency, may not match AES's widespread adoption and standardization. Ultimately, the choice of encryption algorithm should be guided by specific application requirements, balancing security, performance, and compatibility considerations.

REFERENCES

[1] Radhi, S. M., & Ogla, R. (2023). In-Depth Assessment of Cryptographic Algorithms Namely DES, 3DES, AES, RSA, and Blowfish. Iraqi Journal of Computers, Communications, Control and Systems Engineering, 23(3), 125-138.

[2] Azeez, N. A. (2018). Comparative analysis of encryption algorithms. Covenant Journal of Informatics and Communication Technology.

[3] Olutola, A., & Olumuyiwa, M. (2023). Comparative analysis of encryption algorithms. European Journal of Technology, 7(1), 1-9.

[4] Ebrahim, M., Khan, S., & Khalid, U. B. (2014). Symmetric algorithm survey: a comparative analysis. arXiv preprint arXiv:1405.0398.

[5] Sood, R., & Kaur, H. (2023). A literature review on rsa, des and aes encryption algorithms. Emerging Trends in Engineering and Management, 57-63.

[6] Rihan, S. D., Khalid, A., & Osman, S. E. F. (2015). A performance comparison of encryption algorithms AES and DES. International Journal of Engineering Research & Technology (IJERT), 4(12), 151-154.

[7] Ogundoyin, I. K., Ogunbiyi, D. T., Adebanji, S., & Okeyode, Y. O. Comparative Analysis and Performance Evaluation of Cryptographic Algorithms.

[8] Riman, C., & Abi-Char, P. E. (2015). Comparative analysis of block cipher-based encryption algorithms: a survey. Information Security and Computer Fraud, 3(1), 1-7.

[9] Anwar, M. N. B., Hasan, M., Hasan, M. M., Loren, J. Z., & Hossain, S. T. (2019). Comparative study of cryptography algorithms and its' applications. International Journal of Computer Networks and Communications Security, 7(5), 96-103.

[10] Gupta, A., & Walia, N. K. (2014). Cryptography Algorithms: a review. International Journal of Engineering Development and Research, 2(2), 1667-1672.

[11] Soni, A. K., Kumar, G., Kumari, P., Nayak, A., & Arpita, A. (2023). Comparative Analysis of Cryptographic Algorithms in Computer Network (No. 10218). EasyChair.

[12] Hercigonja, Z. (2016). Comparative analysis of cryptographic algorithms. International Journal of Digital Technology & Economy, 1(2), 127-134.

[13] AlRoubiei, M., AlYarubi, T., & Kumar, B. (2020, June). Critical analysis of cryptographic algorithms. In 2020 8th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-7). IEEE.

[14] Ubochi, C., Olaniyi, B., Ukagwu, K., & Nnamchi, S. (2023). A Comparative Analysis of Symmetric Cryptographic Algorithm as a Data Security Tool: A Survey. Journal of Science and Technology Research, 5(3).

[15] https://en.wikipedia.org/wiki/Encryption

[16] Commey, D., Griffith, S., & Dzisi, J. (2020). Performance comparison of 3DES, AES, Blowfish and RSA for Dataset Classification and Encryption in Cloud Data Storage. International Journal of Computer Applications, 177(40), 17-22.

[17] Jassim, S. A., & Farhan, A. K. (2022). Designing a New Lightweight AES Algorithm to Improve the Security of the IoT Environment. IRAQI JOURNAL OF COMPUTERS, COMMUNICATIONS, CONTROL AND SYSTEMS ENGINEERING, 22(2), 96-108.

[18] Dulla, G. L., Gerardo, B. D., & Medina, R. P. (2018, November). An Enhanced BlowFish (eBf) Algorithm for Securing x64FileMessage Content. In 2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM) (pp. 1-6). IEEE.

[19] ALattar, I. M., & Rahma, A. M. S. (2021). A comparative study of researches based on magic square in encryption with proposing a new technology. IRAQI JOURNAL OF COMPUTERS, COMMUNICATIONS, CONTROL AND SYSTEMS ENGINEERING, 21(2), 102-114.

[20] Harini, M., Pushpa Gowri, K., Pavithra, C., & Selvarani, M. P. (2017). Comparative study and analysis of various Cryptographic Algorithms. Int J Sci Eng Res, 8(5), 2229-5518.

[21] Gaur, S. S., Kalsi, H. S., & Gautam, S. (2019). A comparative study and analysis of cryptographic algorithms: RSA, DES, AES, BLOWFISH, 3-DES, and TWOFISH. International Journal Of Research In Electronics And Computer Engineering (IJRECE), 7(1), 996-999.

[22] Dibas, H., & Sabri, K. E. (2021, July). A comprehensive performance empirical study of the symmetric algorithms: AES, 3DES, Blowfish and Twofish. In 2021 International Conference on Information Technology (ICIT) (pp. 344-349). IEEE.

[23] Assa-Agyei, K., & Olajide, F. (2023). A Comparative Study of Twofish, Blowfish, and Advanced Encryption Standard for Secured Data Transmission. International Journal of Advanced Computer Science and Applications, 14(3), 393-9