ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25feb1650

A Comparative Study of Symmetric Encryption Algorithms and Techniques for Enhancing Smartphone Security

C.V. Mbamala[1]; M.O Onyesolu[2]; G.N Ezeh[3];
U.V Maduabuchi[4]; C.N Onyechi [5]; C.D Anyiam[6]

[1;3]Department of Information Technology, Federal University of Technology, Owerri Owerri, Nigeria
[2]Department of Computer Science, Nnadi Azikiwe University, Awka, Nigeria
[4]Department of Computer Education, Federal College of Education (Technical) Umunze
[5]Department of Computer Science Chukwuemeka Odumegwu Ojukwu University Anambra state. Nigeria
[6]Department of Computer Science, Federal University of Technology, Owerri, Nigeria

Publication Date: 2025/03/18

Abstract: The increasing reliance on smartphones has heightened the need for robust data security. Symmetric cryptography, recognized for its efficiency and speed, plays a crucial role in safeguarding data on mobile devices. This study evaluates the performance of selected symmetric encryption algorithms, DES, 3DES, AES, Twofish, and Blowfish on smartphones. The algorithms were tested for encryption time, decryption time, and avalanche effect using file sizes of 1000KB, 2000KB, 3000KB, 4000KB, and 5000KB. The avalanche effect was also assessed for each algorithm with block sizes and key sizes tailored to their specifications. The results reveal that AES and Twofish exhibit the lowest encryption and decryption times, particularly for large files, demonstrating superior efficiency. For avalanche effect, AES achieved 53.9063%, surpassing the critical 50% threshold, followed by 3DES (50%), Blowfish (46.875%), Twofish (46.094%), and DES (23.4375%). AES strikes an optimal balance between speed and security, making it the most suitable encryption algorithm for smartphone applications

Keywords: *Smartphones, Security, Encryption, Decryption, Cryptography, Symmetric, Block Cipher.*

How to Cite: C.V. Mbamala; M.O Onyesolu; G.N Ezeh; U.V Maduabuchi; C.N Onyechi ; C.D Anyiam (2025). A Comparative Study of Symmetric Encryption Algorithms and Techniques for Enhancing Smartphone Security. *International Journal of Innovative Science and Research Technology*, 10(2), 2313-2319. https://doi.org/10.38124/ijisrt/25feb1650

I. INTRODUCTION

In today's digital age, smartphones have become indispensable, serving as the primary medium for communication, financial transactions, social networking, and accessing both personal and corporate data. As these devices grow more advanced, they store vast amounts of sensitive information, making them prime targets for cyber threats [1]. Consequently, the demand for robust security measures is more critical than ever, with encryption emerging as one of the most effective methods for safeguarding smartphone data. Encryption transforms data into an unreadable format, accessible only to authorized users with the correct decryption key [4]. This ensures confidentiality, data integrity, and user privacy. Given the widespread use of mobile applications, cloud storage, and constant internet connectivity, smartphone encryption is essential for reducing vulnerabilities to cyberattacks [3].

Unlike encryption on desktops or servers, smartphone encryption poses unique challenges [1]. One of the key issues is balancing security with performance. Many smartphones, particularly older or budget models, operate under resource constraints such as limited processing power, battery life, and storage capacity. Therefore, encryption algorithms must be optimized to minimize performance overhead and energy consumption while maintaining strong security.

This study seeks to determine the most efficient encryption algorithm for smartphones by evaluating its encryption and decryption performance and assessing security through the avalanche effect. An algorithm that achieves an avalanche effect greater than 50% is generally considered secure and resistant to cryptanalysis attacks that exploit predictable patterns. Faster encryption and decryption not only enhance efficiency but also reduce CPU usage, leading to lower power consumption. This is particularly beneficial for applications that frequently encrypt data, such as messaging

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25feb1650

apps and file managers, as shorter processing times help minimize background energy drain.

In addition to encryption and decryption performance, this research also examines the selected algorithms based on key factors such as key size, number of rounds, plaintext block size, and scalability. This comprehensive evaluation provides a thorough assessment of their effectiveness and suitability for smartphone encryption.

II. REVIEW OF RELATED WORKS

This subsection reviews and analyzes previous studies on the comparison of various encryption algorithms, highlighting gaps in existing literature.

Logunelo et al. [6] compared the performance of DES, AES, and EB64 encryption algorithms on a mobile phone, focusing on encryption and decryption times with SMS plaintext. They found that EB64 was significantly faster than both AES and DES for SMS encryption. However, their study was limited to small SMS file sizes, highlighting a knowledge gap regarding how these algorithms perform with larger files, such as images and videos. Our research will close the gap by exploring the algorithms' performance with larger file sizes, which are more typical in real-world mobile applications

Amalraj and Raybin [4] conducted a comprehensive review of cryptography techniques, including AES, DES, 3DES, Blowfish, and RSA. Given the increasing frequency of online transactions, data security has become paramount. The authors surveyed existing research on encryption techniques and evaluated the performance of selected symmetric algorithms. Their findings concluded that Blowfish outperformed other algorithms in terms of performance. However, the study didn’t measure the security of the selected algorithms.

Alenzi [2] conducted a Java-based simulation to evaluate the performance of AES, Blowfish, RC2, RC4, RC6, DES, Deseed, SEED, XTEA, and IDEA. The simulation tested encryption speed, throughput, and CPU utilization for file sizes ranging from 1MB to 1GB. The results indicated that RC4 and AES were the top performers in terms of encryption and decryption speed. However, AES was considered a more suitable candidate due to its superior security level. However, the study did not validate the security result of the algorithms, which is a critical aspect of cryptographic analysis

A-Shabi [4] conducted a comparative study on important algorithms in terms of speed (implementation) and security (special keys) using difference metrices. The comparative results showed the strength and weakness of symmetric and asymmetric. According to their result AES is the most reliable in speed encryption, decoding, length of key, structure and usability. However, the study did not provide details on the sample size used for the experiments, which limits the ability to fully assess the robustness of the findings.

Elminaam et al. [5] compared the performance of six symmetric encryption algorithms (AES, DES, 3DES, RC2, Blowfish, and RC6) under different settings. They found that RC6 was the fastest algorithm for varying packet sizes, but RC2, RC6, and Blowfish were slower for image data. 3DES was slower than DES. Larger key sizes, especially for AES and RC6, led to increased battery and time consumption. How the study did not explicitly evaluate the security of the algorithms, a crucial element of cryptographic analysis.

Alabdulrazzed et al. [6] provided an overview of widely used encryption algorithms, detailing their mechanisms and key features. The algorithms compared included AES, Blowfish, RC2, RC4, RC6, DES, Triple DES, SEED, XTEA, and IDEA. Performance metrics were assessed based on encryption speed, throughput, and CPU utilization across various file sizes, from 1MB to 1GB. Findings indicated that RC4, RC6, and AES delivered the best results in terms of encryption time and throughput. However, the study did not assess the security of the selected algorithms, which limits a comprehensive understanding of their overall effectiveness.

Alanazi et al. [8] conducted a comparative analysis of three encryption algorithms DES, 3DES, and AES based on nine factors, including key length, cipher type, block size, security level, and the number of possible keys at a rate of 50 billion keys per second. The study concluded that AES outperforms DES and 3DES in overall security and efficiency. However, it did not assess the encryption and decryption times of the algorithms, leaving a gap in understanding their practical performance.

Roo and Harpret [9] carried out a comprehensive study on the security of RSA, DES and AES algorithms. According to the results of their survey, AES algorithm is more efficient in terms of speed, time, throughput and avalanche effect. However, the study did not provide experimental results to substantiate these claims, limiting the ability to validate their conclusions fully.

Hendi et al. [3] conducted a comparative study of three encryption algorithms RSA, DES, and AES by examining key parameters such as computation time, memory usage, and output size, all of which are critical for evaluating an algorithm's efficiency. Their findings revealed that DES had the fastest encryption time, while AES consumed the least memory, with only a minor difference in speed between AES and DES. In contrast, RSA exhibited the slowest encryption time and the highest memory usage, though it produced the smallest output size. Notably, the study did not include a direct assessment of the algorithms' security, an essential aspect of cryptographic effectiveness.

Pavithra et al. [7] evaluated multiple cryptographic algorithms by analyzing parameters such as processing time across video files of varying sizes (ranging from 1 MB to 1100 MB) and in different formats (.vob and .dat) at various processing speeds. They measured both encryption and decryption times for each file. The results demonstrated that AES outperformed DES and Blowfish by requiring less processing time and achieving higher throughput. However, the study did not include a direct assessment of the algorithms' security, a critical component of cryptographic analysis.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25feb1650

Mandal et al. [10] compared the two widely used symmetric encryption algorithms, Data Encryption Standard (DES) and Advanced Encryption Standard (AES), focusing on the avalanche effect resulting from a one-bit change in plaintext, memory requirements, and encryption simulation time. The results show that AES exhibits a significantly higher avalanche effect than DES, while DES consumes more memory and takes longer to simulate. This demonstrates AES's superior performance and suitability for secure message encryption, such as chat communications, and for transactions involving financial exchanges. However, the study did not assess the encryption and decryption times of the selected algorithms.

Mohammad et al. [12] surveyed DES, 3DES, AES, and HiSea, focusing on their different design methodologies. The evaluation considered parameters such as encryption and decryption time, memory usage, and throughput. Based on the performance assessment, Blowfish, AES, and HiSea were found to provide higher security, depending on the available resources. However, the study did not evaluate the security of the selected algorithms, which limits a comprehensive assessment of their overall effectiveness in protecting data.

III. SYMMETRIC ALGORITHMS AND TECHNIQUE

- *Data Encryption Standard (DES)*

The Data Encryption Standard (DES) is a symmetric-key encryption algorithm developed by IBM in the 1970s and adopted as a federal standard in 1977. It uses a 56-bit key and encrypts data in 64-bit blocks through 16 rounds of substitution and permutation, based on the Feistel network structure [3].

- *3DES or Triple Data Encryption Standard*

Triple DES (3DES) is an enhanced version of the outdated Data Encryption Standard (DES), designed to address the vulnerabilities of DES's 56-bit key. It applies DES encryption three times to each data block, effectively creating a 168-bit key, which increases security [5]. However, 3DES is slower than newer encryption methods due to its triple encryption process and remains vulnerable to brute-force attacks because of its small data block size. Despite these limitations, 3DES was introduced to overcome DES's weak key length by using up to three unique keys for encryption.

- *Advanced Encryption Standard (AES)*

The Advanced Encryption Standard (AES) is a symmetric-key encryption algorithm adopted by the U.S. government in 2001, replacing the older Data Encryption Standard (DES). Developed by Belgian cryptographers Joan Daemen and Vincent Rijmen, AES is based on the Rijndael cipher and uses a block size of 128 bits. It supports three key lengths, AES-128 (128-bit key, 10 rounds), AES-192 (192-bit key, 12 rounds), and AES-256 (256-bit key, 14 rounds), providing varying levels of security. AES operates using a Substitution-Permutation Network (SPN) structure, applying transformations such as substitution, permutation, mixing, and XOR operations with the key. Known for its high security, AES has been extensively tested and is the global encryption standard used in government, financial, and commercial sectors for securing sensitive data [9].

- *Twofish*

Twofish is a symmetric-key block cipher created by Bruce Schneier and his team in the late 1990s as a candidate for the AES competition [11]. Although it was not selected, it remains a strong and secure algorithm. Operating on 128-bit data blocks, Twofish supports key sizes of 128, 192, or 256 bits, allowing for varying levels of security. It uses a Feistel structure to process data through multiple rounds, where each round applies specific transformations, ensuring both efficiency and security.

- *Blowfish*

Blowfish is a symmetric-key block cipher designed by Bruce Schneier in 1993 as a fast and secure alternative to DES. It encrypts data in 64-bit blocks and supports key lengths from 32 to 448 bits [12]. Using a Feistel network, Blowfish operates in 16 rounds, applying key-dependent transformations. Its simplicity and efficiency make it suitable for embedded systems and resource-constrained environments. Though not broken, Blowfish has a relatively small block size, leading to its successor, Twofish, addressing some of its limitations.

IV. METHODOLOGY

An android encryption application called secret space file encryptor (SSE) was implemented on our smartphone. SSE supports a variety of encryption standards, while the application primarily focuses on AES, it also enables users to experiment with other algorithms such as Blowfish, Twofish, DES, 3DES and other customizable ciphers. The encryption application was implemented on Infinix Smart X6511B with android 11, 2.00 GB RAM, and 32.00 GB ROM, a mid-ranged device chosen for its affordability, relevance in developing regions, and suitability for testing resource-constrained scenarios. Plaintext sizes ranging from 1000 KB to 5000 KB were used to simulate real-world applications, enabling a comprehensive analysis of scalability, efficiency, and security for each algorithm. This methodology highlighted the strengths and weaknesses of the algorithms under typical smartphone usage conditions.

V. RESULTS AND DISCUSSION

The results will be presented in two sections: a comparison of the results and findings from the experimental analysis.

A. Comparison

After reviewing the algorithms and their definitions and specifications, Table 1. provides a concise comparison of DES, 3DES, AES, Twofish, and Blowfish, focusing on factors such as the number of rounds, key size, block size, architecture, security, and scalability.

B. Experimental Analysis

The study carried out two separate experiments: one assessed the avalanche effect to evaluate the security of the

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25feb1650

algorithms, and the other measured the encryption and decryption times of the five selected algorithms.

➢ *Avalanche Effect*

The avalanche effect in cryptography refers to a desirable property of encryption algorithms (especially block ciphers and hash functions) where a small change in the input (such as flipping a single bit) results in a significant, unpredictable change in the output. We conducted this experiment using various block sizes and key sizes that are compatible with the algorithms under study as presented on table 2. The following steps were used to calculate the avalanche effect of the selected algorithms.

- Encrypt plaintext P1 using key K1 to produce ciphertext C1.
- Flip one bit in the plaintext (or key) to create P2 (or K2).
- Encrypt the modified plaintext (or key) to produce ciphertext C2
- Convert C1 and C2 into binary format.
- Count the number of differing bits between C1 and C2.
- Calculate Avalanche Percentage using the formula

$$AF = \frac{\text{No of change bits in ciphertext}}{No\ of\ bits\ in\ cipher\ text} X\ 100 \quad (1)$$

Table 1 Comparative results of DES, 3DES, AES, Twofish, and Blowfish.

Algorithm	No of rounds	Key size(bits)	Block size (bits)	Architecture	Security rate	Speed	Scalability
DES	16	56	64	Feistel	Inadequate	Slow	No
3DES	48	112|168	64	Feistel	Secure	Very slow	Yes
AES	10,12,14	128, 192,256	128	Substitution and permutation	Secure	Fast	Yes
Two fish	16	128,192 or 256	128	Feistel	Moderate	Fast	Yes
Blowfish	16	32- 448	64	Feistel	Moderate	Fast	Yes

From the comparison, on table 1 we observed that the AES algorithm stands out as the best symmetric cipher due to its robustness, speed, scalability, and availability in multiple versions, making it well-suited to meet smartphone requirements. Twofish provides strong security and moderate performance, making it a viable alternative for applications where security is critical. Blowfish performs well for smaller data sizes but lacks robustness for modern encryption needs due to its small block size while DES and 3DES are outdated and unsuitable for smartphones due to security vulnerabilities and high resource consumption in the case of 3DE

Table 2 Presents the Avalanche effect Results in Percentage for the Five Selected Algorithms.

Algorithms	Secret key	Plaintext	Plaintext (Hex)	Ciphertext	Avalanche effect
DES	ABCDEFG (56 bits)	Secureme (64 bits)	53454355 52454D45.	68ae9c51f0848d33fh	$\frac{15}{64}X100 = 23.4375$
		Securema (64 bits)	53656375 72656D61	ae2a6abf g43ad	
3DES	16g43ay67b gsu7wtds6gr (168bits)	Secureme (64 bits)	53454355 52454D45	eacbf3f5a86cef453	$\frac{32}{64}X100 = 50.$
		Securema (64 bits)	536563757 2656D61	797fgabc4b536a3	
AES	2b7e151628ae2a6abf 7158809cf4f3cr (128 bits)	MySecretdata (128 bits)	4d79536563 72657444617461	68ae9c51f0848d33f52 2f53cc62b7baf	$\frac{69}{128}X100 = 53.9063$
		MySecretDatb (128 bits)	4d795365637 2657444617462	68ae9c51f0848d33f52 2f53cc62b7baa	
TWOFISH	2b7e151628ae2a6abf 7158809cf4f3cr (128 bits)	MySecretdata (128 bits)	4d79536563726 57444617461	68ae9c51f0848d33f52 2f53cc62b7baf	$\frac{59}{128}X100 = 46.094$
		MySecretDatb (128 bits)	4d79536563726574 44617462	68ae9c51f0848d33f52 2f53cc62b7baa	
BLOWFISH	Tg4d (32bits)	Secureme (64 bits)	5345435552 454D45	564df43abfda653bc	$\frac{30}{64}X100 = 46.875$
		Securema (64 bits)	68ae9c51f0848d33f 522f53cc62b7baa	76bdaf5328edac64	

From the result of avalanche effect presented in table 2, AES (53.9063%), AES shows the strongest diffusion, with an avalanche effect exceeding the critical threshold of 50%. This indicates that AES effectively spreads changes in the plaintext across the ciphertext, making it highly resistant to cryptanalysis techniques like differential and linear cryptanalysis.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25feb1650

3DES (50%)-3DES surpasses the 50% mark, demonstrating robust diffusion. However, its performance is slightly weaker than AES, reflecting its older design. While it still provides strong security, 3DES is less efficient compared to modern algorithms and is being phased out in favor of AES.

Blowfish and Twofish exhibit avalanche effects below the ideal 50%, though they are close. These results indicate that while these algorithms offer reasonable diffusion, they might be less resistant to advanced cryptanalysis than AES or 3DES.

DES (23.4375%) - Lowest Avalanche Effect: DES demonstrates very poor diffusion, with an avalanche effect significantly below the 50% threshold. This result highlights DES's vulnerability to cryptanalysis and reinforces its status as an obsolete encryption standard unsuitable for modern applications.

➢ *Experimental Analysis of Encryption and Decryption Time*

Using the installed SSE application, encryption and decryption were performed on file sizes of 1000KB, 2000KB, 3000KB, 4000KB, and 5000KB. The operation times were measured in seconds and converted to milliseconds. The encryption and decryption times for each algorithm were recorded, with Table 3 presenting a summary of the results.

Table 3 Results of Encryption and Decryption

File size (KB)	ENCRYPTION/ DECRYPTION TIME (m/s)	ALGORITHMS				
		DES	3DES	AES	TWOFISH	BLOWFISH
1000	Encryption	4,662	4853	3332	3101	3092
	Decryption	4667	4957	3337	4107	4077
2000	Encryption	5227	5440	4232	4151	4282
	Decryption	5000	5221	4300	4445	4607
3000	Encryption	6006	6049	4942	5101	5377
	Decryption	6270	6400	5007	5392	5479
4000	Encryption	7492	7800	5730	5900	5013
	Decryption	7499	8100	5998	6033	6096
5000	Encryption	8114	8602	6330	6510	6667
	Decryption	8223	8990	6508	6806	6998

Based on the encryption and decryption times presented in table 3, 3DES has the highest decryption time, underscoring its inefficiency and making it unsuitable for modern applications that handle large file sizes. AES and Twofish emerge as the most efficient algorithms, particularly for larger files, where their decryption times remain consistently low. Blowfish is slightly less efficient than AES and Twofish for larger file sizes, but it still outperforms DES and 3DES. DES demonstrates moderate efficiency, performing better than 3DES but considerably slower than AES and Twofish. Overall, lower encryption and decryption times enhance efficiency, conserve energy, and improve scalability and usability. Figures 1 and 2 clearly illustrate the results of encryption and decryption, respectively.

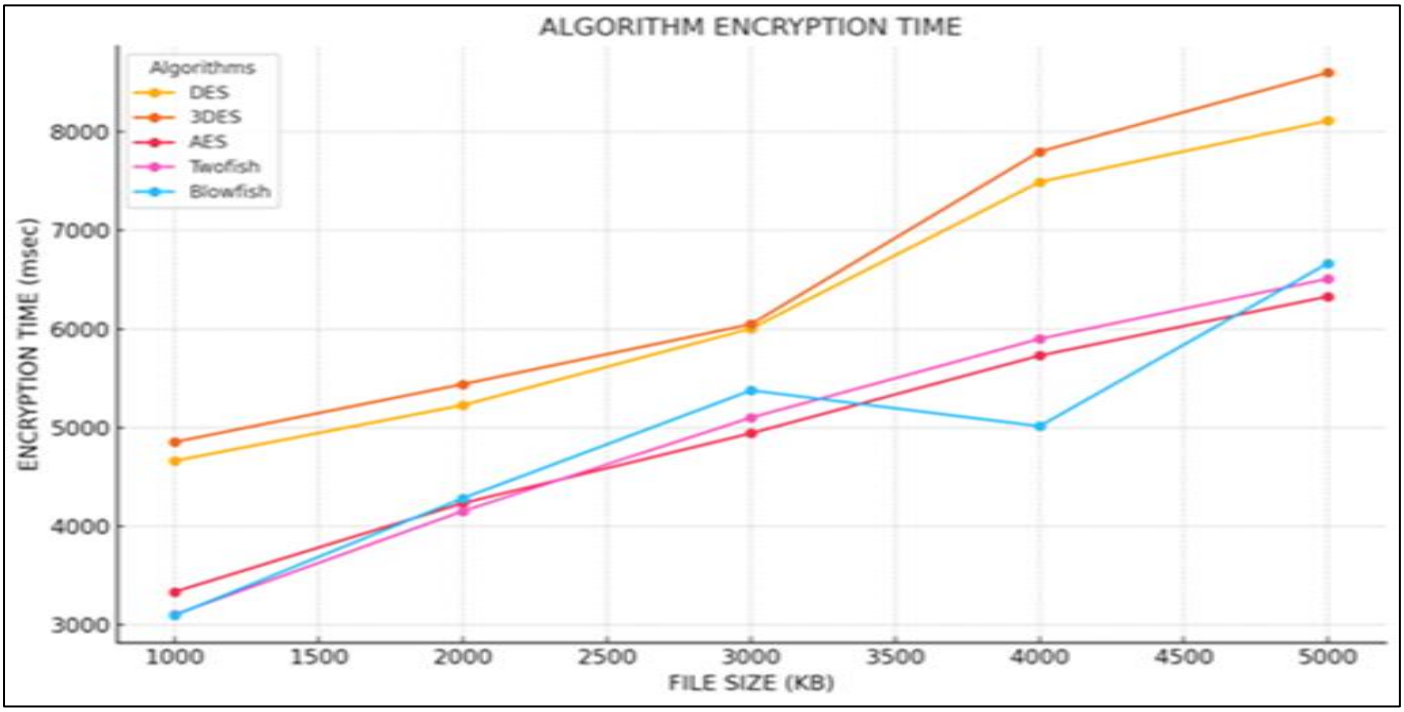

Fig 1 Encryption time of DES, 3DES, AES, TWOFISH and BLOWFISH.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25feb1650

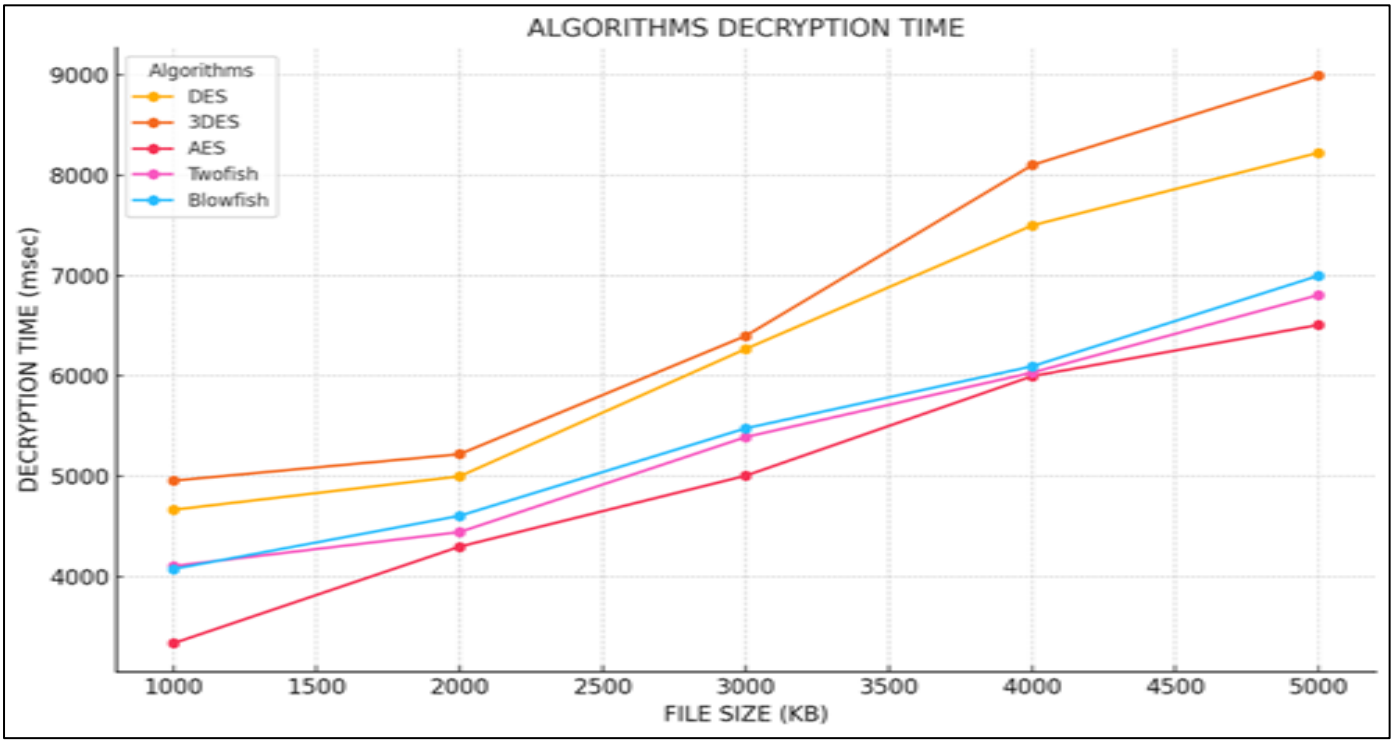

Fig 2 Decryption time of DES, 3DES, AES, TWOFISH and BLOWFISH

VI. CONCLUSION AND RECOMMENDATION

This study conducted a comparative analysis of five symmetric encryption algorithms AES, Twofish, Blowfish, 3DES, and DES to evaluate their efficiency and suitability for smartphones. The evaluation was based on key performance indices, including encryption time, decryption time, and avalanche effect.

The findings indicate that AES is the most efficient algorithm for smartphones, demonstrating the lowest encryption and decryption times and achieving an avalanche effect above the critical 50% threshold, ensuring strong security and excellent performance. Twofish and Blowfish also showed competitive results, with moderate encryption and decryption times and acceptable avalanche effects, making them viable alternatives.

3DES, while achieving a good avalanche effect, was hindered by its significantly slower encryption and decryption times, reflecting its inefficiency for resource-constrained devices like smartphones. DES performed poorly across all metrics, confirming its obsolescence as a secure encryption standard.

For smartphone encryption, AES is strongly recommended due to its superior balance of speed, energy efficiency, and security, making it ideal for modern mobile applications. Twofish and Blowfish may be considered as alternatives in scenarios where AES is unavailable or custom implementations are required. 3DES and DES should be avoided due to their inefficiencies and security limitations, which render them unsuitable for smartphones.

Future work could explore optimizing AES and Twofish for energy-efficient encryption tailored specifically to mobile platforms.

REFERENCES

[1]. Arora, P., Singh, A., and Tyagi, H. (2021). Evaluation and comparison of security issues on cloud computing environment. *World of Computer Science and Information Technology Journal* (WCSIT), 2(5), 179-183

[2]. Alenezi, M.N., Haneen, A., and Nada, Q.M. (2020). Symmetric

[3]. encryption algorithms: Review and evaluation study. *Iraqi Journal of Science*, 12(1), 104-109.

[4]. Hendi, A., Dwariri M., and Quadi, Z. (2019). A novel simple and highly secure method for data encryption-decryption. Journal of communication Network and International security, 11(1), 232-238.

[5]. M-shabi, M.A, (2019). A survey of symmetric and Asymmetric cryptography algorithms in information security. *International Journal of scientific Research publication*, 9(3), 576-589.

[6]. Elminaam, D. S. A., Kader, H. M. A., and Hadhoud, M. M. (2023). Performance evaluation of symmetric encryption algorithms. *International Journal of Computer Science and Network Security*, 8(12), 280-286.

[7]. Longunleko, K.B., Aeniji, O.D., and Lonuneleko, A.M. (2020). A comparative study of symmetric cryptography mechanism on DES, AES and EB64 for information security. *International Journal of Scientific Research in Computer Science and Engineering*, 8(1), 45-51.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25feb1650

[8]. Pavithra, S, and Ramadevi, D, (2019), Performance evaluation of symmetric algorithm. *Journal of Mathematical and Computing Science*, 2(8), 67-73.

[9]. Alanazi, H., Zaidan, B. B., Zaidan, A. A., Jalab, H. A., Shabbir, M., and Al-Nabhani, Y. (2023). New comparative study between DES, 3DES and AES within nine factors. *International Journal of Computer Science and Network Security*, 4(1), 56-65.

[10]. Beniwal, T. and Deepak, P. (2020). Enhancement in AES algorithms. *International Research Journal of Engineering and Technology*,9(2), 423-427.

[11]. Roo, P.A., and Harpreet, K. (2023). A literature review on RSA, DES and AES encryption algorithm. *Emerging Trends in Engineering and Management*, 2(5), 57-63.

[12]. Mandal, A. K., Parakash, C., and Tiwari, A. (2019). Performance evaluation of cryptographic algorithms: DES and AES. *In IEEE Students Conference on Electrical, Electronics and Computer Science,* 12-14 October 2019, (pp. 1-5). Australia: IEEE.

[13]. A., Singh, M. L., and Bansal, P. K. (2018). Comparison of various encryption algorithms and techniques for secured data communication in multi-node network. *International Journal of Engineering and Technology*, 7(3), 89-95.