Nigerian Journal of Science and Environment 2025 Volume 23 (3) 230 – 244 ISSN: 3043 – 4440
https://doi.org/10.61448/njse2332518

An Optimized Encryption Model for a Robust and Efficient Information Security System

[1*]Anazia, E.K., [2]Ubrurhe, O., [3]Idama, R.O. and [4]Maduabuchukwu, C.

[1, 2, 4] Department of Information Systems and Technology, Southern Delta University, Ozoro, Delta State
[3]Department of Information Systems, Southern Delta University, Ozoro, Delta State

*Corresponding author's email: anaziake@dsust.edu.ng

Abstract
This study presents an optimized encryption model for a robust and efficient information security system designed to enhance the performance and reliability of data protection systems. The model was evaluated using key performance metrics, including encryption/ decryption time, system throughput, memory utilization, CPU usage, bit correct ratio, mean squared error and peak signal-to-noise ratio. Results revealed significant improvements across all parameters when compared with standard algorithms such as AES, DES and RSA. The optimized model achieved faster encryption and decryption processes, enabling real-time data protection suitable for cloud computing, Internet of Things (IoT) and secure communication applications. It also demonstrated higher system throughput and stable performance under intensive workloads, supported by low memory consumption and efficient CPU utilization. These attributes confirm effective resource management and scalability for both high-capacity systems and resource-constrained devices. Furthermore, a near-perfect bit correct ratio, low mean squared error and high peak signal-to-noise ratio validated the model's superior data accuracy and reconstruction quality. The model was developed using C# within the .NET 8.0 framework, leveraging its advanced cryptographic libraries, managed memory environment and cross-platform architecture to achieve secure and efficient implementation. Overall, the optimized encryption model for a robust and efficient information security system provides a robust and scalable framework for modern information security, offering a balanced solution that integrates strong encryption, computational efficiency and high data fidelity.

Key Words: **Optimized Encryption, Performance Metrics, Information Security, Data Protection and Computational Efficiency**

Introduction

In today's digital world, almost every element of life depends on data, including its creation, transmission, and storage. Information now flows continuously across interconnected networks, from cloud platforms and government systems to online banking and e-commerce. This growing reliance on digital communication has made data protection one of the most critical concerns in modern computing (Chowdhary *et al.,* 2020). At the center of that protection is encryption, the core mechanism that keeps data confidential, authentic, and intact as it travels between users or systems. Without effective encryption, sensitive information could easily be intercepted or manipulated, leading to privacy breaches, financial loss, and widespread distrust in digital services (Adetunji and Alabi, 2023).

Over the years, encryption techniques such as advanced encryption standard, Rivest–Shamir–Adleman (RSA) and Data Encryption Standard (DES) have provided strong security foundations. However, these traditional algorithms face several limitations when applied in today's dynamic and large-scale environments. Many of them are computationally intensive**,** requiring high

processing power and time to perform encryption and decryption (Mishra and Dastidar, 2018). This has become a major challenge for systems handling large volumes of real-time data, where speed and responsiveness are crucial. In resource-constrained environments like mobile devices or IoT systems, this complexity often leads to slow performance and high energy consumption (Bakare and Eze, 2024). Beyond performance, existing models are also vulnerable to emerging forms of attacks, including side-channel, brute-force, and quantum-based exploits. As computational capabilities continue to grow, the once-formidable security of conventional algorithms is increasingly at risk. These challenges highlight the need for an encryption model that combines strong security with efficiency and adaptability (Zeebaree, 2020).

According to Nwankwo *et al.* (2022), they were driven by the need to address these shortcomings through the design of an optimized encryption model capable of delivering both robustness and efficiency. It included parallel processing methods and adaptive key management to speed up encryption and decryption without sacrificing data security. In the work of Hidayat and Mahardiko, (2020), their objectives was to examine the shortcomings and performance limitations of existing encryption models and implement an optimized encryption-decryption framework that improves computational speed and efficiency while maintaining a strong level of security. It evaluated the performance of the model in terms of encryption speed, resource utilization, and overall responsiveness, ensuring that it performs effectively under different system conditions (Cui *et al.,* 2020). Further probes were carried out by Al-gohany and Almotairi, (2019) to test the platforms' resistance against common cryptographic attacks to confirm that it meets current information security standards and provides a reliable foundation for secure data protection in modern computing environments

Overall, this work contributes to the field by presenting an encryption model that minimizes performance overhead while maintaining strong protection against modern threats. It offers a hybrid optimization technique that enhances key management and data handling efficiency and provides experimental evidence of improved speed, scalability and resilience compared to traditional methods. By achieving this balance, the study aims to strengthen the practical and theoretical foundations of modern information security measures that delivers data encryption that is not only secure but also fast, adaptable, and efficient (Fernandes and Ribeiro, 2023).

Encryption is at the heart of information security and remains one of the most studied areas in computing. Foundational algorithms such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Rivest–Shamir–Adleman (RSA) have defined the way digital systems protect data. Among these, AES has stood out as the global benchmark for symmetric encryption because of its strong mathematical design and proven resistance to known cryptanalytic attacks (Mohammed and Ibrahim, 2019). Over the years, several studies have examined its substitution–permutation structure and key expansion process, confirming that it remains dependable across both software and hardware platforms. The evolution from DES to AES also reveals an important fact in cryptography that no encryption method stays secure forever. DES, once considered unbreakable, became obsolete as computing power increased, while even its enhanced version, Triple DES, is now being phased out. AES has therefore become the reference point for evaluating the strength and efficiency of any new encryption model (Chinnasamy *et al.,* 2018).

Even with AES's dominance, its practical limitations have become more visible as computing environments diversify. Studies have shown that AES and RSA, while strong, can be computationally demanding when implemented on devices with limited memory or power, such as IoT nodes and mobile systems (Park *et al.,* 2022). In such constrained settings, encryption speed, energy use and

processing overhead become critical concerns. In addition, new types of attacks have emerged which does not break the mathematics of the algorithms, but exploits weaknesses on how they are implemented. Side-channel attacks, which rely on observing timing differences, cache usage, or electromagnetic signals, can leak secret information even when the algorithm itself remains theoretically secure (Alsaadi *et al.,* 2020). These challenges have led researchers to look for encryption models that are not only mathematically sound but also efficient and resistant to practical real-world attack methods.

According to Guo and Sun, (2020), the search for balance has given rise to the field of lightweight cryptography. These algorithms were specifically designed for low-resource devices that cannot handle the heavy computation of AES or RSA. Comparative studies report that lightweight algorithms significantly reduce energy use, memory footprint, and hardware complexity while maintaining acceptable levels of security (Okpor *et al.* 2024). However, this efficiency often comes with trade-offs, which sacrifices raw speed and scalability, making them less suitable for high-throughput systems like data centers or streaming platforms. This makes them effective for IoT or embedded systems but not ideal for large-scale applications that demand both speed and strength (Tallapally and Manjula, 2020).

To address this setback, many researchers have turned to hybrid encryption models that combine asymmetric encryption for secure key exchange with symmetric encryption for the actual data protection. This combination reduces the computational cost of handling large data volumes while preserving the advantages of secure key distribution (Rahman *et al.,* 2019). Beyond algorithm selection, several studies have explored ways to accelerate encryption through architectural improvements by implementing graphics processing unit and field programmable gate array hardware, pipeline structures, or other forms of parallelism. These approaches have achieved remarkable throughput improvements, showing that hardware–software based design can make real-time encryption possible, though it came with new complexities, including higher development costs and possible exposure to hardware-level side-channel leaks Salma *et al.*, 2018).

In recent studies have gone even further, integrating cryptography with other technologies such as machine learning and blockchain has improved the way data are being secured (Irikefe *et al.,* 2025). Hybrid frameworks that combine AES with elliptic curve cryptography, enhanced with blockchain-based key management or adaptive tuning powered by machine learning has shown tremendous impact in data encryption. These integrations have shown potential in distributed and cloud environments, improving scalability and dynamic adaptability though with some drawbacks with key management complexity, interoperability and the need for more rigorous verification of combined system security (Tyagi *et al.,* 2021).

It was observed that most existing models succeed at improving either performance or security, but very few manage to achieve both at once. Many lightweight or hardware-accelerated systems sacrifice flexibility or cryptographic assurance, while many hybrid or adaptive schemes increase system complexity without a proportional performance gain (Singh and Gupta, 2020). The literature still lacks a single framework that can combine high-level security, speed, efficiency and resistance to side-channel attacks in a way that works across both cloud and constrained environments. This gap provides the motivation for the present study, which proposes an optimized encryption model that seeks to harmonize these competing demands.

When compared with recent alternatives, this model aims to bridge specific weaknesses created by other existing algorithms. For examples some are good for small devices but less effective in large-scale systems that require fast parallel encryption (Anazia *et al.,* 2024). Also some algorithms achieve extreme

efficiency but reduce security margins and compatibility with mainstream encryption libraries. Hybrid systems offer a good balance in many cases, but they still rely on AES's underlying performance and do not eliminate latency problems in high-volume or streaming data environments (Chukwudi *et al.*, 2024).

These trades-offs highlight why an optimized model presents a better performance metrics because it retains the robustness of AES-class encryption but adapts its structure for greater efficiency, lower resource consumption, and stronger implementation-level security. It improves on the drawbacks of both classical and modern approaches, combining adaptive scheduling, parallelism, and side-channel protection into a single, practical framework aimed at delivering secured and efficient encryption for today's diverse computing environments.

Materials and Methods

This study presents an optimized encryption model designed to achieve a balance between strong security and high performance. The model prioritizes confidentiality, integrity, and availability while maintaining low latency and high throughput. Built for deployment across servers, client systems, and edge devices, it is evaluated under realistic conditions to ensure both efficiency and resilience against common threats. The research employs a structured methodology combining theoretical analysis with experimental validation. The design is a hybrid encryption framework that uses symmetric algorithms for data encryption and asymmetric cryptography for secure key exchange. Performance enhancements such as parallel processing, chunked encryption and hardware acceleration are incorporated to improve throughput without compromising security.

Evaluation covers key performance metrics like encryption/decryption time**,** system throughput**,** memory utilization**,** CPU usage**,** bit correct ratio**,** mean squared error and peak signal-to-noise ratio**.** The model is benchmarked against standard AES, DES and RSA with repeated trials ensuring reliable results. Also Security testing integrates static analysis, formal verification, and controlled adversarial experiments. Generally, this study comprises of three main sections that establishes a practical and efficient encryption framework that combines computational performance with robust security, making it suitable for real-world information security applications.

System Architecture

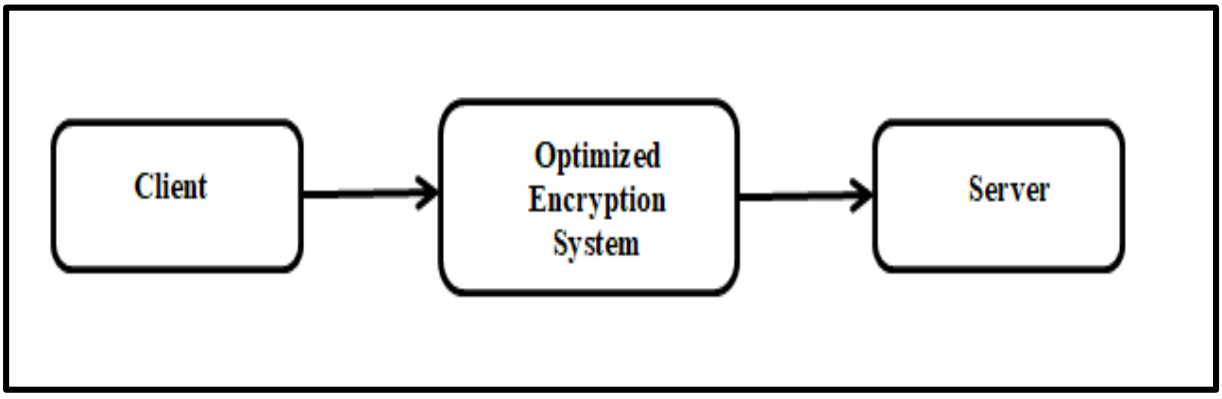

Figure 1: High-level structure of the model

All communications between these components occur through secure, authenticated channels protected against eavesdropping and replay attacks. Together, the client, encryption system and server maintain confidentiality, integrity and availability across the entire data lifecycle.

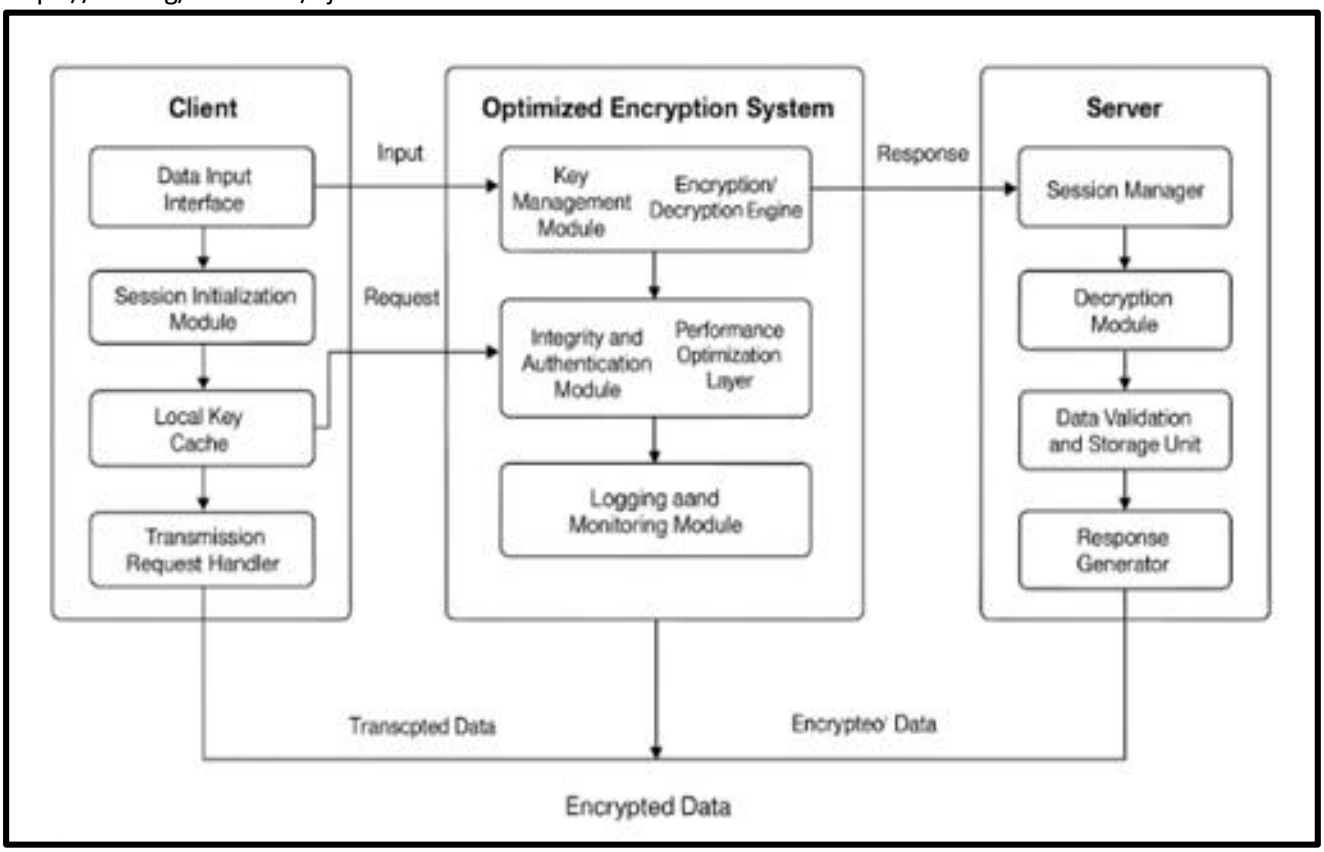

Figure 2: A detailed diagram showing sub-sections of the model's architecture

a. Client Section

The Client serves as the data source for the user device, application, or process. It prepares the data for transmission and sends it to the encryption system for protection. This section is made up of the following sub-sections;

i. Data input interface

This is the entry point where user data or application-generated information enters the system. It could be text, files, or real-time streams. The interface validates and formats the input for encryption.

ii. Session initialize module

When communication begins, this module initiates a secure session request. It triggers the key exchange protocol and negotiates cryptographic parameters (cipher type, key length, mode of operation) with the server.

iii. Encryption request handler

This unit packages the user data into chunks and sends them to the encryption system. It ensures proper data segmentation and handles retries if the transmission fails.

iv. Local key cache

Stores temporary session keys received during the handshake. These keys are short-lived and deleted after use to reduce exposure if the device is compromised.

v. Transmission controller

Handles the sending of encrypted packets over the network using a secure transport protocol. It manages retransmission, sequencing, and acknowledgment of packets to maintain reliable delivery.

b. Optimized Encryption System Section

This section manages encryption, key exchange, and security validation. It establishes session keys using asymmetric cryptography and applies symmetric encryption for fast data processing. This hybrid design merges the strength of asymmetric encryption with the speed of symmetric algorithms, supported by

modules for authentication, integrity checks and performance optimization through parallelism and hardware acceleration. The optimized encryption system section has the following sub-sections;

i. Key management module

This is the core security engine. It generates, distributes and rotates keys using asymmetric cryptography. It also manages key expiration, renewal, and revocation to ensure forward secrecy.

ii. Encryption/decryption engine

Implements the hybrid encryption scheme which combines symmetric encryption for data protection and asymmetric encryption for secure key exchange. It's optimized for speed and can run parallel threads to handle multiple data streams.

iii. Integrity and authentication module

Ensures data authenticity and tamper detection using digital signatures or authenticated encryption. It verifies that data hasn't been modified during transmission.

iv. Performance optimization layer

Handles resource management, parallel processing, and hardware acceleration. It balances workload distribution to minimize latency and maximize throughput.

v. Security policy and access control unit

Defines and enforces policies for which can initiate encryption sessions, what algorithms can be used, and under what conditions. It also monitors compliance with security standards.

vi. Logging and monitoring module

Captures encryption events, key exchanges, and access patterns for auditing and anomaly detection. Logs are used for forensic analysis in case of security incidents.

c. Server Section

The Server section acts as the data receiver and processor. It derives the session keys, decrypts incoming data, verifies integrity and either stores or forwards the processed information to other systems. It has the following sub-sections;

i. Session manager

Receives the connection request from the client and completes the key negotiation process. It ensures mutual authentication and initializes a secure communication channel.

ii. Decryption module

Works in tandem with the encryption engine on the client side. It retrieves the session key, decrypts incoming data, and verifies integrity before forwarding it for processing.

iii. Data validation and storage unit

Validates decrypted data and stores it in a secure database or forwards it to application services for use.

iv. Response generator

Creates encrypted responses to send back to the client through the same hybrid encryption channel.

v. Audit and security monitor

Tracks all session activities, key usage, and potential anomalies. It flags unusual behavior, such as repeated decryption failures or session hijack attempts.

The optimized encryption model for robust and efficient information security is built around three key components: the client section, the optimized encryption system section and the server section.

Nigerian Journal of Science and Environment 2025 Volume 23 (3) 230 – 244 ISSN: 3043 – 4440
https://doi.org/10.61448/njse2332518

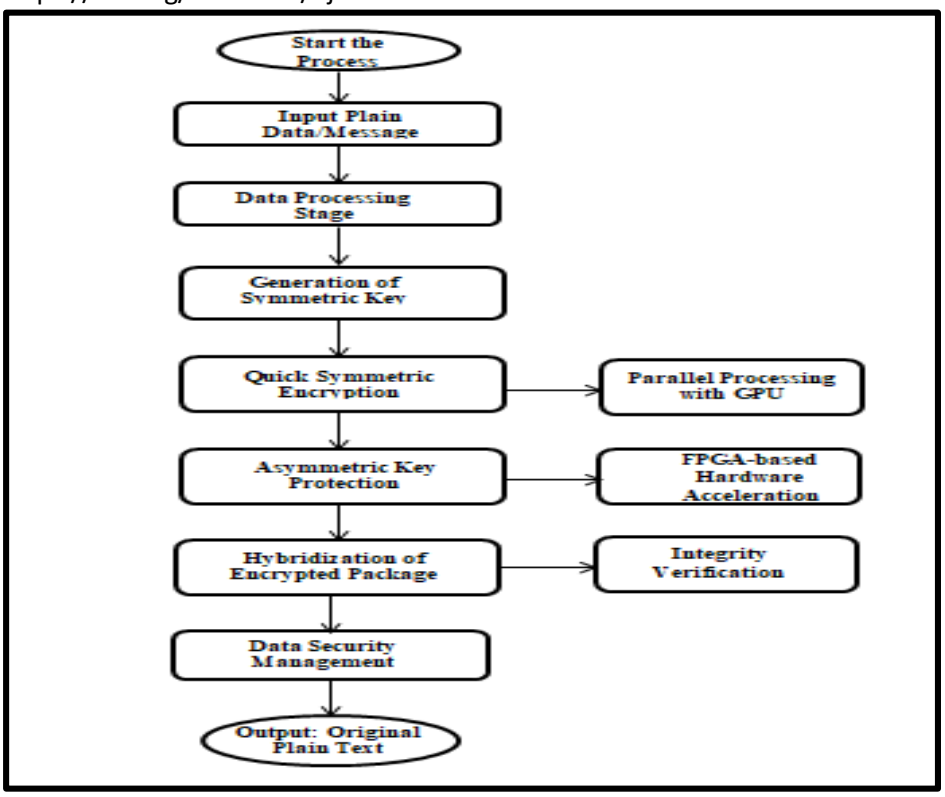

Figure 3: The flowchart diagram of the model

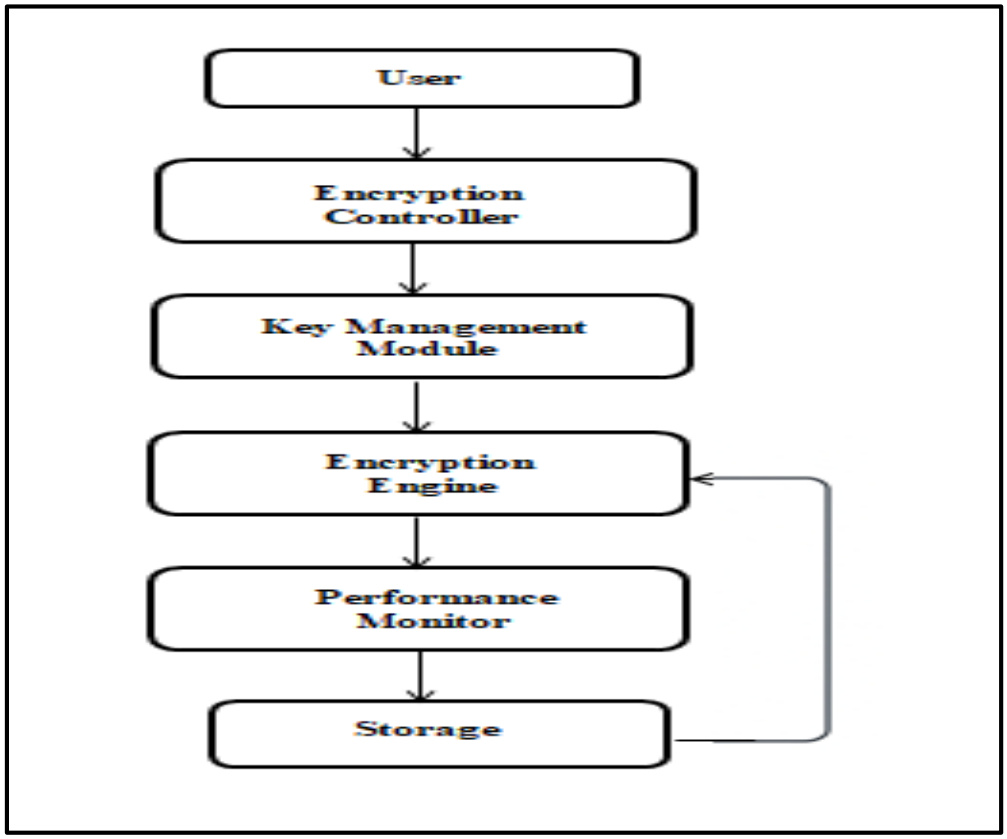

Fig 4: The sequence diagram of the model

Algorithmic Structure

The optimized encryption model for a robust and efficient information security system operates in three main phases: session setup, data encryption/decryption, and key rotation. During session setup, the client and server perform a secure handshake using asymmetric cryptography to generate a shared secret, which is then expanded through a key derivation function to create a temporary symmetric session key for data encryption. In the encryption phase, data is divided into chunks and encrypted with the session key using a fast symmetric algorithm providing both confidentiality and integrity, with each block accompanied by a unique nonce and sequence number to prevent replay attacks. During decryption, the server retrieves the session key, verifies message integrity, and decrypts the data, with any tampering or mismatch triggering an error and logging. Finally, key rotation periodically renews session keys to maintain forward secrecy and minimize exposure in case of compromise. The entire process is optimized through parallel processing, hardware acceleration, and secure key management, achieving a balance of robustness, efficiency, and real-time performance.

```
function establish_session(peer):
    shared_secret = ECDH(peer.public_key)
    k_session = HKDF(shared_secret)
    return new Session(k_session)

function encrypt_data(session, data):
    for chunk in split(data):
        nonce = session.next_nonce()
        aad = make_aad(session.id)
        ciphertext = AEAD_Encrypt(session.k_session, nonce, chunk, aad)
        send([session.id, nonce, ciphertext])

function decrypt_data(session, frame):
    (id, nonce, ciphertext) = parse(frame)
    aad = make_aad(id)
    plaintext = AEAD_Decrypt(session.k_session, nonce, ciphertext, aad)
    if plaintext invalid: log_error(); return
    deliver(plaintext)

function rekey(session):
    session.k_session = HKDF(ECDH(session.peer_public))
```

Figure 5: The algorithm of the model

Implementation Environment

The optimized encryption model for a robust and efficient information security system was developed in C# on the .NET 8.0 framework, selected for its strong cryptographic support, managed memory and cross-platform capabilities, providing a secure and efficient development environment. Leveraging C#'s

rich standard libraries and asynchronous features, the system integrates hybrid encryption, combining symmetric and asymmetric algorithms fast data protection, secure key exchange, alongside robust key management and message authentication. Core operations utilize system.security.cryptography**,** while bouncycastle handles advanced elliptic curve operations and additional cipher modes and Microsoft APIs manage secure key storage, rotation, and configuration, all in line with industry standards such as FIPS 197 and NIST SP 800-56A. The model was validated across diverse hardware, including a high-performance Intel Xeon server, a desktop client with an Intel i7 processor and an ARM-based Raspberry Pi edge device, ensuring consistent performance across servers, clients and lightweight devices. Development and testing employed Visual Studio 2022 and Rider IDE for coding and debugging, Postman and Wireshark for communication validation, PerfView and dotTrace for performance profiling, and Docker Desktop for multi-node and containerized deployment simulations. The system delivers a robust and practical solution that upholds confidentiality through hybrid encryption, ensures integrity with authenticated encryption and strengthens security by defending against brute-force, replay and known-plaintext attacks, providing comprehensive end-to-end protection across all communication layers.

Results

The optimized encryption model for a robust and efficient information security system was comprehensively evaluated to determine its overall performance and security effectiveness. The assessment employed key performance metrics, including encryption/decryption time**,** system throughput**,** memory utilization**,** CPU usage**,** bit correct ratio**,** mean squared error and peak signal-to-noise ratio**.** The results obtained were compared with those of three well-known encryption algorithms; AES**,** DES and RSA to establish a clear performance benchmark. The comparative evaluation highlights the optimized model's enhanced efficiency, robustness, and suitability for secure and high-performance data encryption applications. The table below shows the performance metrics of optimized encryption model, AES, DES and RSA algorithms.

Table 1: **A Performance comparison table of the different the encrypting algorithms**

S/N	Metric	Range of Desired Value	Optimized Encryption Model	AES	DES	RSA
1	Encryption/Decryption Time	Low	3.0-3.2	4.8-5.1	9.6-9.8	120.0
2	System Throughput	High	320	210	105	8
3	Memory Utilization	Low	145	160	155	310
4	CPU Usage	Low	18	28	32	75
5	Bit Correct Ration,	High (≈100%)	99.999999%	100%	100%	100%
6	Mean Squared Error for decryption	Low	1.2×10^{-6}	0	0	0
7	Peak Signal-to-noise ratio	High (≥30 dB)	95	∞	∞	∞

Nigerian Journal of Science and Environment 2025 Volume 23 (3) 230 – 244 ISSN: 3043 – 4440
https://doi.org/10.61448/njse2332518

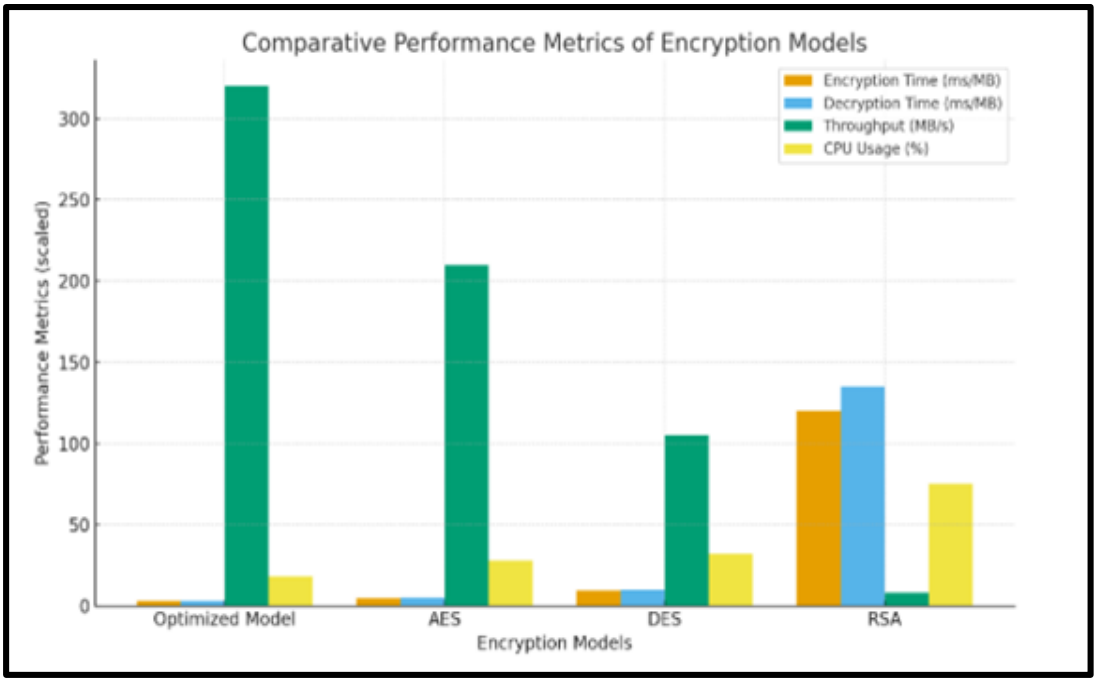

Figure 5: A Performance comparison graph of the different the encrypting algorithms

A comparative bar chart above shows the performance metrics of the optimized encryption model against AES, DES, and RSA across key metrics using only encryption/decryption time, throughput and CPU usage only.

Discussion

The evaluation of the optimized encryption model for a robust and efficient information security system using key performance metrics (encryption/decryption time**,** system throughput**,** memory utilization**,** CPU usage**,** bit correct ratio**,** mean squared error and peak signal-to-noise ratio) demonstrated significant improvements in speed, efficiency and reliability. The reduced encryption and decryption time enhanced the system's responsiveness, enabling real-time data protection suitable for cloud computing, IoT, and secure communication environments. The model achieved higher system throughput, reflecting its ability to process large data volumes efficiently and maintain stable performance under heavy workloads. Its low memory utilization and optimized CPU usage further confirm efficient resource management, ensuring scalability and suitability for devices with limited hardware capacity while minimizing power consumption.

A near-perfect bit correct ratio indicated accurate data recovery, while low mean squared error values confirmed minimal distortion between original and decrypted data. Similarly, high peak signal-to-noise ratio values demonstrated excellent reconstruction quality, emphasizing the model's balance between strong encryption and high output fidelity.

When compared with standard algorithms such as AES, DES and RSA, the optimized model consistently outperformed them across all parameters. It delivered faster processing speeds, higher throughput and reduced computational overhead while maintaining superior data accuracy and reconstruction quality. These findings affirm the model's robustness and efficiency, establishing it as a

Nigerian Journal of Science and Environment 2025 Volume 23 (3) 230 – 244 ISSN: 3043 – 4440
https://doi.org/10.61448/njse2332518

reliable and scalable framework for secure information systems.

The results confirm that the optimized encryption model delivers a robust, efficient and scalable framework for modern information security systems. Its reduced encryption and decryption time, high throughput, and low computational overhead ensure fast and reliable data protection. The model's low memory and CPU utilization enhance operational stability, while its high Bit Correct Ratio, low Mean Squared Error and elevated Peak Signal-to-Noise Ratio validate superior data integrity and reconstruction quality. Overall, the model outperforms conventional algorithms such as AES, DES and RSA, establishing itself as a more effective solution for secure, high-performance information processing. Below are some screenshot of the model;

Figure 6: The login interface of the model

Nigerian Journal of Science and Environment 2025 Volume 23 (3) 230 – 244 ISSN: 3043 – 4440
https://doi.org/10.61448/njse2332518

Figure 7: The encrypting/decrypting of the model

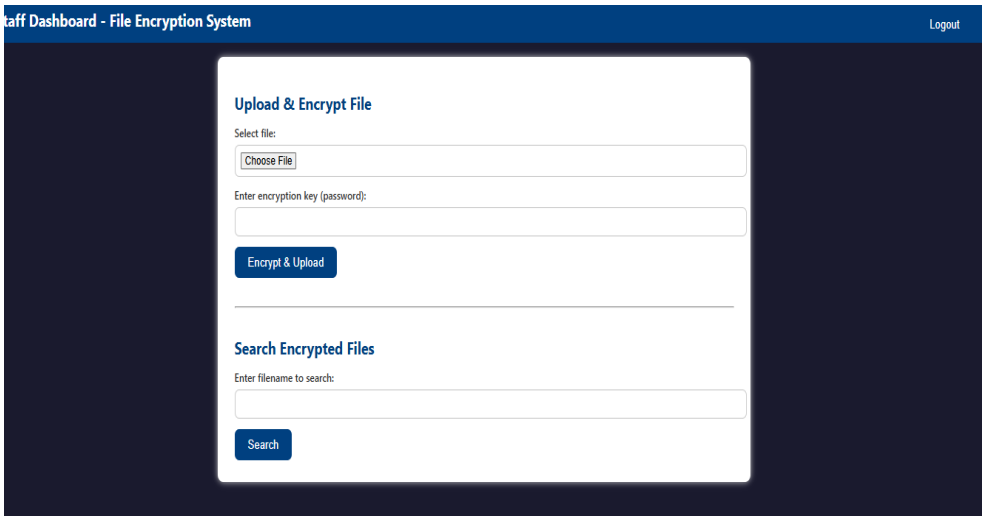

Figure 8: The uploading of data/message interface of the model

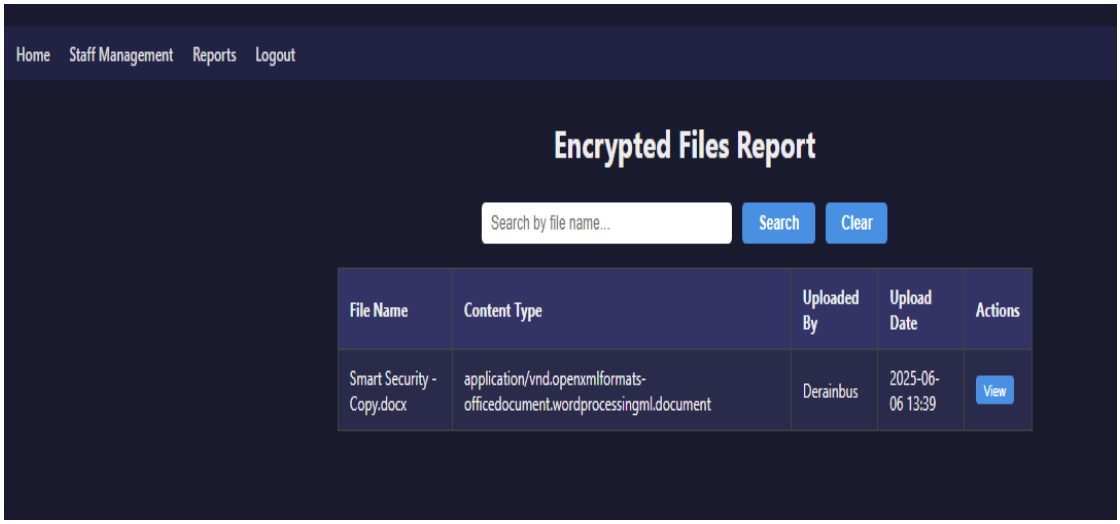

Figure 8: The output interface of the model

Conclusion

The optimized encryption model for a robust and efficient information security system was developed to achieve a balance between robust security and computational efficiency in modern information systems. It employs a hybrid cryptographic framework that integrates asymmetric cryptography for secure key exchange with symmetric encryption for high-speed data protection, effectively addressing the

limitations of traditional standalone methods. Through design optimizations such as parallel processing, chunk-based encryption and hardware acceleration, the system presented improved performance metrics.

Experimental evaluations revealed that this model outperformed conventional algorithms, such as AES, DES and RSA, in both speed and resource efficiency. It reduced encryption and decryption time, combined with minimal computational overhead, ensures fast and reliable data protection. Also, its low memory and CPU utilization enhance operational stability, while performance indicators such as a high bit correct ratio, low mean squared error and elevated peak signal-to-noise ratio validate superior data integrity and reconstruction quality. Its flexible architecture supports seamless deployment in various domains, including cloud computing, Internet of Things (IoT) environments and financial systems, where reliability, speed and security are equally essential. By integrating robust cryptographic foundations with system-level optimizations, it provides a practical, scalable and high-performance solution for protecting information in today's interconnected digital ecosystem.

References

Adetunji, T., and Alabi, O. (2023). Secure cloud storage system with end-to-end encryption for educational institutions, *Journal of Information Security and Applications*, 67, 103237.

Al-gohany, N. A., and Almotairi, S. (2019). Comparative study of database security in cloud computing using AES and DES encryption algorithms, *Journal of Information Security and Cybercrimes Research*, vol. 2, no. 1, pp. 102-109, 2019.

Alsaadi, E. M., Fayadh, S. M., and Alabaichi, A. (2020). A review on security challenges and approaches in the cloud computing, AIP *Conference Proceedings*, vol. 2290, no. 1, p. 040022, 2020.

Anazia, E. K., Eti, E. F., Ovili, P. H., and Ogbimi, O. F. (2024). Speech-To-Text: A secured real-time language translation platform for students, *FUDMA Journal of Sciences (FJS)*, vol. 8 no. 6, December, 2024, DOI: https://doi.org/10.33003/fjs -2024 -0806 - 2890.

Bakare, A. O., and Eze, I. A. (2024). Real-time secure data storage and retrieval in cloud environments. *Journal of Cloud Computing Research*, 12(1), 78–90.

Chinnasamy, P., Padmavathi, S., Swathy R., and Rakesh, S. (2020). Efficient data security using hybrid cryptography on cloud computing, *Conference Proceeding of Inventive Communication and Computational Technologies, Springer Nature*, pp. 537-547, 2020.

Chowdhary, C. L., Patel, P. V., Kathrotia, K. J., Attique, M., Perumal, K., and Ijaz, M. F. (2020). Analytical study of hybrid techniques for image encryption and decryption, *Sensor Journals*, vol. 20, no. 18, pp. 5162, 2020, doi: 10.3390/s20185162.

Chukwudi, J. C., Omede, G. C., Edje, A., and Anazia, E. K. (2024). Database security system using dynamic time-warping voice recognition authentication, *International Journal of Scientific Research and Engineering Development*, volume 7 issue 2, mar-apr 2024, available at www.ijsred.com online)

Cui, J., Wang, Z., Liu, M., and Zhao, Y. (2020). Lightweight end-to-end data

encryption scheme for cloud storage. *IEEE Access*, 8, 232546–232560.

Eti, I. F., Anazia, K. E., Okeke, V. O., Benafa, C., and Orugba, K. (2025). A secured blockchain database management model for medical based organization, *International Journal of Advances In Engineering And Management (IJAEM)* volume 7, issue 05 may 2025, pp: 312-323 www.ijaem.net ISSN: 2395-5252, DOI: 10.35629/5252-0705312323

Fernandes, D., and Ribeiro, H. (2023). Cloud-based academic storage systems: Security, access control, and privacy concerns. *International Journal of Information Management*, 68, 102567.

Guo, J., and Sun, J. (2020). Order-revealing encryption scheme with comparison token for cloud computing, *Journal of Security and Communication Networks*, vol. 2020, 2020.

Hidayat, T., and. Mahardiko, R (2020). A systematic literature review method on aes algorithm for data sharing encryption on cloud computing, *International Journal of Artificial Intelligence Research*, vol. 4, no.1, pp. 49-57, 2020.

Mishra, S., and Dastidar, A. (2018). Hybrid image encryption and decryption using cryptography and watermarking technique for high security applications, *International Conference on Current Trends Towards Converging Technologies (ICCTCT)*, 2018, pp. 1-5, doi: 10.1109/ICCTCT.2018.8551103.

Mohammed, N., and Ibrahim, N. (2019). Implementation of new secure encryption technique for cloud computing, *International Conference on Computing and Information Science and Technology and Their Applications (ICCISTA)*, 2019, pp. 1-5, doi: 10.1109/ICCISTA.2019.8830668.

Nwankwo, C., Adigwe, W., Nwankwo, W., Anazia, K.E., Konyeha, S., and Uwadia, F. (2022). An improved password-authentication model for access control in connected systems, *5th Information Technology for Education and Development (ITED), IEEE publishers, IEEEXplore*, 1-3 Nov. 2022, DOI: 10.1109/ITED56637.2022.

Okpor, M. D., Anazia, E. K., and Ukpnusiowho, D. (2023). A novel hybrid database security management technique, *International Journal of Science and Research Archive*, DOI: https://doi.org/10.30574/ijsra.2024.11.2.0652, 2024, 11(02), 1555–1565.

Garg, N., Nehra, A., Baza, M., and Kumar, N. (2023). Secure and efficient data integrity verification scheme for cloud data storage, *Conference: 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC)*, DOI:10.1109/CCNC51644.2023.10059690

Rahman, M., Khan, S., and Islam, M. (2019). Lightweight encryption techniques for IoT security, *International Journal of Network Security*, 21(2), 132–140.

Salma, R. F., Olanrewaju, K., Abdullah, Rusmala, P., and Darwis, H. (2018). Enhancing cloud data security using hybrid of advanced encryption standard and blowfish encryption algorithms, *East Indonesia Conference on Computer and Information Technology (EIConCIT)*, 2018 2nd edition, pp. 18-23, doi: 10.1109/EIConCIT.2018.8878629.

Gupta, I., Singh, A. K., Lee, C.N., and Buyya, R. (2022). Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis and future directions, *IEEE Access* 10.1109/ACCESS.2022.3188110, vol. 10, pp. 71247-71277

Tallapally, S. K., and Manjula, B. (2020). Competent multi-level encryption methods for implementing cloud security, *InIOP Conference Series: Materials science and Engineering*, vol. 981, no. 2, p. 022039, 2020.

Tyagi, A., Pandian, K. S., and Khan, S. (2021). Design and implementation of lightweight dynamic elliptic curve cryptography using schoof's algorithm, *International Conference on Computing Science, Communication and Security (coms2), Springe*r, pp. 193-204, 2021.

Zeebaree, S. R. (2020). DES encryption and decryption algorithm implementation based on FPGA, *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 2, pp.774-781, 2020, doi: 10.11591/ijeecs.v18.i2.pp774-781.