Researchers Journal of Science and Technology (REJOST)
https://rejost.com.ng

Comparative Analysis of Different Multilevel States for Four Notable Cryptographic Schemes

Joel N.Ugwu*, Stephen A.Mogaji, Seye E. Akinsanya, John O. Awoyemi and Jeremiah C. Obi

Received: February 10, 2024 /Accepted: April 3, 2024

Abstract

Multilevel cryptography refers to the use of multiple layers of encryption algorithms and keys to protect sensitive data and communications. The output of the encryption at the first layer becomes an input to the second encryption algorithm. The output of the second encryption algorithm becomes an input to the third encryption algorithm, and so on until the desired layers are satisfied. Suchamultileveled approach might be implemented using the same or different encryption algorithms.In this article, we conducted an extensive examination of different possible combinations of symmetric-key (Advanced Encryption Standard, (AES) and Digital Encryption Standard, (DES)) and asymmetric-key (Rivest, Shamir, and Adleman cryptography, (RSA) and Elliptic-Curve Cryptography, (ECC)) cryptosystems for data encryption and security byusing questionnaires. Comparative assessments of performance, scalability, computational complexity, memory requirements, and hardware optimization capabilities were carried out to identify the strengths and weaknesses in a combined state. Some key performance metrics such as speed, throughput, and resource utilization were determined per scheme implementation using an experimental platform to complement the theoretical analysis. Examinations of known cryptanalytic attacks, susceptibility to quantum attacks, and real-world vulnerability trends evaluated the security resilience of the systems. Factors such as implementation challenges, key management, standardization status, and adoption in practice were considered from an application perspective. A prototype general architecture for multilevel cryptosystem that can withstand any blind cryptanalytic attack was presented. Result shows that there is better performance in terms of encryption and decryption when AES is multileveled with RSA in contrast to DES performance with either RSA or ECC. Furthermore, ECC frequently surpasses RSA in speed for asymmetric cryptographic tasks owing to its utilization of shorter key

lengths to achieve comparable security levels. Nevertheless, real-world performance may fluctuate depending on implementation intricacies and the capabilities of specific hardware. Using multilevel encryption algorithms gives a better assurance to information safety as it shows more proof against cryptanalytic attack.

✉ **Joel N. Ugwu**: joel.ugwu@fuoye.edu.ng; +2348063305810

Department of Computer Science, Federal University, Oye-Ekiti, Nigeria

Keywords: Multilevel encryption; Elliptic-Curve Cryptography; RSA; Digital Encryption Standard; Advanced Encryption Standard; Comparative Analysis

1.0 Introduction

Multilevel cryptography is a security approach that involves different cryptographic estimations and methodologies in a layered manner to overhaul the security of sensitive data and correspondences (Bhaskar and Gopal, 2019). This approach desires to provide more grounded security by joining different cryptographic parts and utilizing their singular assets. In multilevel cryptography, different encryption estimations, key organization methodologies, and access control parts are applied at different levels inside a system or association. Each level tends to a specific layer of security, with its own game plan of cryptographic undertakings and protection measures (Alabi *et al*., 2022). By using various layers of wellbeing endeavors', multilevel cryptography can direct the cut-off points and deficiencies of individual cryptographic plans, achieving a more careful and intense security act.The usage of multilevel cryptography loosens upin various regions where strong security is urgent. It is for the most part used in districts like military correspondences, secure government structures, financial associations, and fundamental establishment confirmation (Godfry, 2019). By using different layers of security, multilevel cryptography spreads out an insurance strategy, decreasing the risk of unapproved access, data breaches, and information leakage. Figure 1 depicts a flowchart of a basic hybrid Cryptosystem.

One of the key justifications for why comparative analysis is fundamental is that there is no one-size-fits-all arrangement in cryptography. Different multilevel cryptographic plans utilize assorted calculations, key administration approaches, and access control instruments, each with its own benefits and limits. Comparative analysis considers a complete assessment of these plans, assisting with distinguishing their one-of-a-kind qualities and capacities (Smith *et al*., 2022). It permits a bewildering a potential open door to survey the reasonableness of every plan for various use cases, applications, and security necessities. Moreover, comparative analysis is associated with the assessment of the introduction of multilevel cryptographic plans. Execution estimations like speed, computational multifaceted design, and adaptability can be overviewed and investigated across different plans. This analysis assists with figuring out the trade-offs between security and computation above, thinking about the decision of the most capable arrangement that meets the best security goals. Cryptography places a strong emphasis on security, and comparative analysis anticipates playing a key role in evaluating the security components of multilevel cryptographic schemes. By pondering different plans as

opposed to various attack vectors, shortcomings, and weaknesses, comparative analysis helps with perceiving their solidarity and security from attacks. This consolidates contemplating the strength of the plans rather than known cryptographic attacks, looking at their key organization parts, and assessing shortcomings in side-channel attacks. Such pieces of information are pressing in making educated decisions about the security position regarding a cryptographic system.

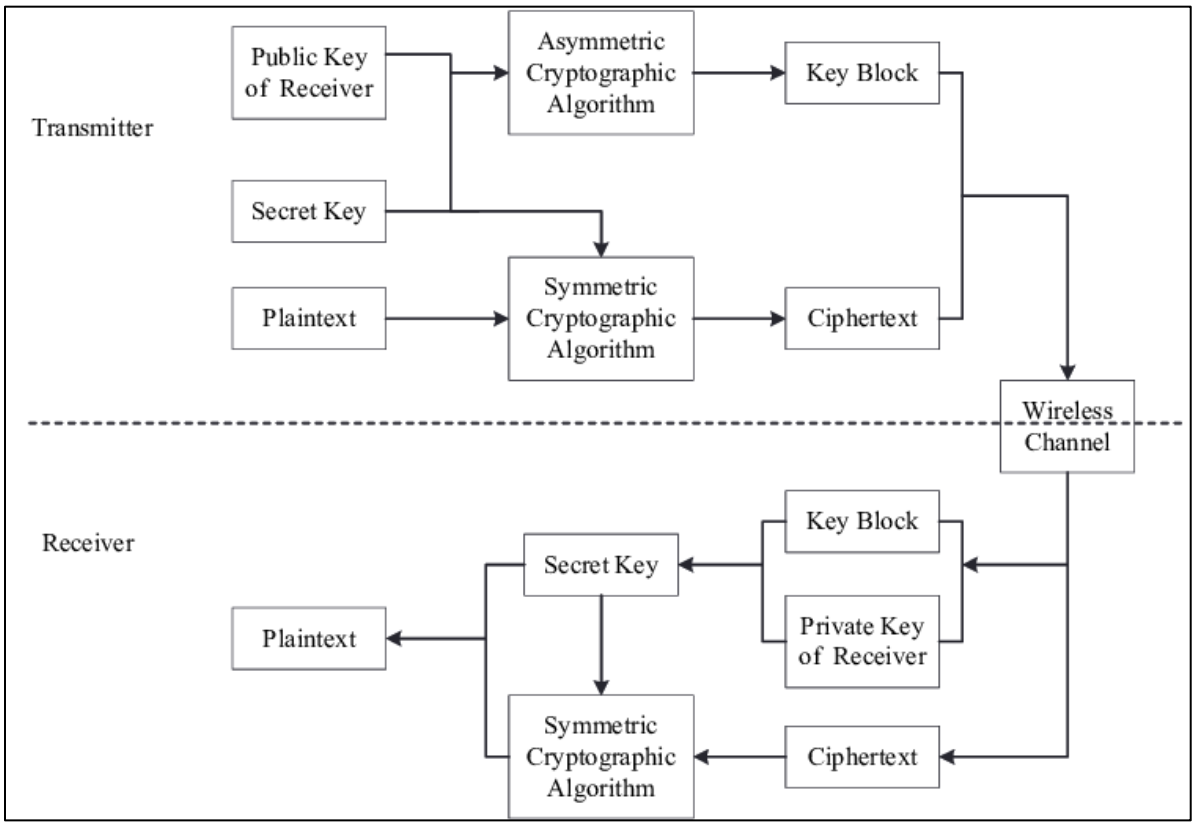

Figure 1: Flowchart of Hybrid Cryptosystem (Chen *et al.*, 2020)

Within the domain of multilevel cryptography, a gap exists in holistic comparative research synthesizing the strengths, vulnerabilities, efficiency, security assurance, and practical deployment factors of different schemes (Vijay *et al.*, 2024).While multilevel cryptography is a promising methodology for further developing information security and secure interchanges, picking a fitting plan for a particular application stays troublesome because of the different scope of accessible plans and their shifting qualities. Consequently, an intentional comparative analysis is supposed to provide a more significant cognizance of various multilevel cryptographic plans, their practicality, and their sensibility for various use cases. This analysis will help trained professionals and specialists in making informed choices and decisions while completing multilevel cryptography, achieving unrivalled security and capability. The goal of this project is to conduct a comprehensive comparative analysis of various multilevel cryptographic plans, assessing their general assets and shortcomings. By thoroughly comparing and examining the security viability, framework execution, and organizational standard of different plans, the

point is to explain their reasonableness for specific applications and use cases.In clear terms, this project tries to progress applied information in the field of multilevel cryptography by furnishing specialists with proof-based direction for choosing ideal plans that accommodate their prerequisites. Generally, by thoroughly looking at and differentiating the capacities and restrictions of various multilevel cryptography arrangements inone next to the other design, the center goal is to illuminate and engage experts and scientists in the same to work on the true execution, designing, and development of cryptographic frameworks. As such, this comparative analysis is expected to act as a complete yet functional dynamic guide for the choice of selection of multilevel cryptographic schemesin real life application such as in the vehicular plate number identification, recognition and storage by various security agencies (Fagbuagun *et al.*, 2020).

2.0 Literature Review

The literature review serves as an essential foundation for the exploration of multilevel cryptographic schemes, offering a comprehensive overview of existing research, methodologies, findings, and gaps within the field. Beginning with the historical evolution of cryptography, the review traces its development from classical to modern techniques, highlighting the pivotal works of pioneers like Claude Shannon and Whitfield Diffie (Jasuja *et al*., 2020). This historical context underscores the transformation of cryptography from a military application to a cornerstone of information security across diverse sectors. Focusing on multilevel cryptographic schemes, a substantial portion of the review delves into seminal research and scholarly articles that define and elucidate the concepts of layered encryption, cascade encryption, and hybrid approaches. This in-depth exploration unveils the underlying principles, cryptographic mechanisms, and operational intricacies of each scheme, shedding light on their contributions to data protection in various contexts. By synthesizing research findings and expert insights, this section presents a holistic understanding of the merits and limitations associated with each approach, setting the stage for a detailed comparative analysis.

The review critically analyzes the strengths, weaknesses, advantages, and disadvantages of the identified multilevel cryptographic schemes. By synthesizing research findings, empirical evaluations, and practical case studies, this analysis provides a nuanced perspective on how each approach fares in real-world implementations and addresses specific security challenges. Additionally, the review delves into potential security threats and vulnerabilities that multilevel cryptographic schemes aim to mitigate, drawing from the field of cryptanalysis to highlight vulnerabilities attackers might exploit and examining how the schemes counteract such threats.

A. Multilevel Cryptographic Schemes

Multilevel cryptographic schemes have emerged as a transformative advancement within the realm of cryptography, providing a heightened level of security and privacy to safeguard sensitive data (Verma and Prasad, 2022). In the following chapter, our exploration delves into the core principles that underpin multilevel cryptography, illuminating its inherent characteristics, while simultaneously embarking on a comprehensive comparison of distinct multilevel cryptographic schemes. At its essence, multilevel cryptography, often interchangeably known as hierarchical or layered cryptography, represents a strategic cryptographic approach that adeptly secures data across varying tiers of sensitivity within organizational systems or broader networks. In

stark contrast to traditional cryptographic methods relying on a single encryption key, multilevel cryptographic schemes introduce a higher level of complexity by employing multiple encryption keys or layers of encryption (Kumar and Saha, 2023). This intricate approach functions as a fortified defence mechanism, enhancing protection against potential breaches and unauthorized access.

At the core of modern cryptography stand pivotal concepts that serve as the cornerstones of secure communication and data protection. Noteworthy among these is public-key cryptography, a ground-breaking concept introduced by Whitfield Diffie and Martin Hellman. This revolutionary approach heralded the era of asymmetric encryption, wherein a pair of distinct keys - a public key for encryption and a private key for decryption - ensure secure and confidential communication even in the presence of potential eavesdroppers. Alongside this, cryptographic hashing, a technique pioneered by Philip Rogaway, enables data to be transformed into a fixed-size hash value. This cryptographic mechanism is indispensable for verifying data integrity and facilitating digital signatures, playing a crucial role in authenticating digital transactions and messages. Collectively, these concepts lay the foundation for establishing secure communication channels that underpin digital interactions.

B. Approaches of Multilevel Cryptographic Schemes

The following are the major approaches of multilevel cryptographic schemes;

i. **Layered Encryption Approach:** The layered encryption approach, a cornerstone of multilevel cryptography, involves the sequential application of multiple encryption layers to a plaintext message or dataset, constituting a robust strategy for bolstering security (Verma and Prasad, 2022). With each encryption layer added, an additional level of complexity and protection is woven into the data, creating formidable barriers against unauthorized access. This method capitalizes on the synergy of diverse cryptographic algorithms and keys, forging a multi-dimensional shield against potential threats. In practice, the layered encryption approach unfolds in a meticulously orchestrated sequence. Beginning with a plaintext, the process ensues: Algorithm A, along with Key A, encrypts the original message into the latter becomes the input for Algorithm B and Key B, engendering. This final encryption layer—carried out by Algorithm C and Key C—yields, the ultimate guarded representation of the original message. The reverse procedure, decryption, follows the reverse order, with each layer decrypted using the corresponding key and algorithm (Kumar and Saha, 2023). However, the implementation of this approach demands a judicious amalgamation of encryption algorithms, precise key management, and a discerning arrangement of encryption layers (Sharma and Dubey, 2017). While layered encryption affords amplified security, potential complexities loom large. Striking a balance between the benefits accrued and the performance costs incurred is paramount. Key management assumes a pivotal role, warranting vigilant safeguarding of individual keys and algorithms to thwart breaches (Chaudhry and Kapoor, 2020).

ii. **Cascade Encryption Approach:** Cascade encryption arises as a transcending stronghold of cryptographic refinement, organizing a fastidious cycle wherein different encryption layers are deftly and successively applied to a plaintext message, coming full circle in a complex, essentially secure ciphertext fortification (Suyal *et al.*, 2017). This unpredictable technique remains a cautious

watchman, an imperturbable sentinel of information security, handily exploring the confounded nexus of different encryption calculations and unmistakable keys to yield a scrambled result that opposes decoding endeavours. As the encryption odyssey begins, the plaintext leaves on a ground-breaking excursion, flowing through a flowing series of encryption organizations, each noticeable by the imprimatur of an exceptional encryption calculation and its harmonious key. This orchestra of cryptographic tasks, fitting the complexities of encryption calculations and keys, makes a song of encryption layers that dance as one, encompassing the first happy in a variegated cover of security. This very troupe of encryption layers adds to the essence of cascade encryption's security worldview, wherein the scrambled result arises as a complex, multi-layered figure text embroidery. This tangled encryption framework dramatically intensifies the intricacy of the code message, making any endeavour to unravel the first message a confounding mission loaded with intricacies. The transaction of encryption layers, coordinated in agreeable progression, winds around an essentially inseparable riddle, confusing still up in the air of cryptographic foes and delivering decoding an impressive test. This perplexing encryption cascade, described by its consistent combination of cryptographic changes, remains a glaring difference to the defined methodology of layered encryption, wherein encryption stages are disengaged layers, frequently particular and freely sustained. Inside the display of information security, cascade encryption arises as a vanguard in settings that request encryption as well as sustained, impenetrable insurance. Hence, cascade encryption is an exceptional combination of hypothetical development and reasonable cryptographic systems, representing the cooperative combination of hypothetical goals and realistic applications chasing information security. This sentinel of safety stands unflinching, carving its heritage across different spaces, spreading out its diverse encryption mantle as a demonstration of the immovable obligation to the security of delicate data in the computerized age.

iii. **Hybrid Approach:** The hybrid encryption approach emerges as a sophisticated synthesis of layered and cascade encryption methodologies, amalgamating their individual strengths to forge a comprehensive defence mechanism against unauthorized access (Verma and Prasad, 2022). This strategic convergence not only accentuates the benefits of both paradigms but also strategically counteracts their inherent limitations, culminating in an intricate and fortified security framework designed to withstand even the most sophisticated cryptographic attacks. In the realm of hybrid encryption, the blending of layered and cascade techniques unfolds with a meticulous orchestration of encryption stages. At its genesis lies the plaintext message, which embarks on a transformative journey. This journey incorporates elements of layered encryption, where the plaintext navigates through successive encryption layers, each endowed with a distinct encryption algorithm and its corresponding key. However, the hallmark of the hybrid approach lies in its seamless transition from one layer to another, akin to cascade encryption. This fusion results in a composite ciphertext structure, embodying both the structured depth of layered encryption and the multi-dimensional complexity characteristic of cascade encryption (Kumar and Saha, 2023).The

benefits inherent to the hybrid approach are manifold and profound. By synergistically amalgamating the attributes of layered and cascade encryption, the hybrid model inherently embodies enhanced security. The fusion of these methodologies creates a multi-layered and multi-dimensional encryption architecture that thwarts adversarial attempts to breach the system's defences. Furthermore, the hybrid approach presents adaptability as a strategic advantage, accommodating diverse threat models and offering a dynamic defence against evolving attack strategies. Unlike single-method encryption, the hybrid approach mitigates the risk of vulnerabilities inherent to a singular methodology, amplifying the overall robustness of the cryptographic framework (Verma and Prasad, 2022).The hybrid encryption approach stands as a testament to the dynamic interplay between cryptographic theory and pragmatic application. It represents a sophisticated response to the evolving challenges of data security, harmonizing innovation and adaptability to safeguard digital interactions, preserve the sanctity of sensitive information, and fortify the foundations of contemporary cryptography.

C. Strengths of Multilevel Cryptographic Schemes

The following are the strengths of multilevel cryptographic schemes:

i. Enhanced Security: Multilevel cryptographic schemes stand as an exemplar of enhanced security through their strategic integration of multiple encryption layers (Verma and Prasad, 2022). This stratification creates a fortified defence architecture, where each layer is fortified by distinct encryption algorithms and keys, culminating in a formidable safeguard against unauthorized access. The additive effect of these layers compounds the complexity of decryption, substantially raising the bar for potential attackers. Each encryption layer necessitates independent decryption efforts, resulting in a time-consuming and resource-intensive process. This inherent intricacy significantly deters brute-force attacks, where attackers must expend substantial computational resources to penetrate each layer sequentially. This layered structure is particularly potent in defending against scenarios where an adversary gains partial access. Even if one layer is compromised, the subsequent layers act as a bulwark, thwarting the adversary's progress and buying valuable time for detection and response (Singh *et al.*, 2024).

ii. Flexibility: Multilevel cryptographic schemes exemplify adaptability, deftly accommodating diverse security requirements and application domains (Kumar et al., 2021). Their modular nature empowers security professionals to tailor encryption strategies to the unique demands of each context. Whether securing financial transactions, medical records, or government communications, multilevel schemes possess the agility to align with the nuanced security mandates of various sectors. The customization of encryption layers to prioritize specific security dimensions—such as confidentiality, integrity, or authentication—ensures that the security architecture remains harmonized with evolving threats and regulatory frameworks. This adaptability renders multilevel schemes a versatile choice for safeguarding data across dynamic and heterogeneous environments (Chaudhry and Kapoor, 2020).

iii. Key Management: Robust key management is a cornerstone of cryptographic systems, and multilevel cryptographic schemes address this requirement with

sophistication. The intricate nature of multilevel architectures demands a meticulous approach to key management. Each encryption layer requires its own dedicated encryption key, thereby diminishing the potential impact of a single key compromise. Key management strategies within multilevel schemes exhibit variability, offering organizations the flexibility to adopt approaches that best suit their operational needs. Hierarchical key management, for instance, streamlines key distribution by deriving lower-level keys from higher-level keys, maintaining a delicate balance between security and efficiency (Chaudhry and Kapoor, 2020). Alternatively, centralized key management systems provide an avenue for seamless administration of encryption keys across multiple layers, bolstering the overall management process.

iv. Comprehensive Data Protection: Comprehensive data protection stands as a cornerstone strength within multilevel cryptographic schemes, where a multi-layered defence strategy is meticulously crafted to address a spectrum of security dimensions. At the core of this strength liesan unwavering commitment to safeguarding data integrity, confidentiality, and authenticity simultaneously. The orchestrated integration of distinct encryption layers not only fortifies data against tampering but also ensures its unaltered and accurate state throughout its lifecycle. This integrity preservation is underpinned by the intricate nature of multilevel schemes, where the need to manipulate multiple layers in concert to compromise data integrity presents an arduous challenge to potential attackers (Almoysheer *et al.*, 2021). Beyond integrity, these schemes also excel in enhancing data confidentiality. The sequential arrangement of encryption layers creates a cascading effect, wherein each layer mandates independent decryption. This intricate sequencing elongates attack lifecycles, granting security teams ample time to detect and counteract intrusion attempts, thus safeguarding confidential information from unauthorized access. Moreover, multilevel schemes contribute to the assurance of data authenticity by embedding cryptographic fingerprints within the encrypted data. This fingerprinting mechanism thwarts attempts at forging or manipulating data without detection, ensuring the trustworthiness of information (Chaudhry and Kapoor, 2020). By encompassing these dimensions, multilevel cryptographic schemes offer a holistic and robust defense mechanism against a diverse array of threats, both internal and external. This comprehensive approach not only bolsters data protection but also cultivates a secure foundation for diverse applications, where the sanctity, trustworthiness, and resilience of sensitive data remain paramount.

D. Weaknesses of Multilevel Cryptographic Schemes

Despite their strengths, multilevel cryptographic schemes also exhibit certain vulnerabilities that warrant consideration. These weaknesses, while not diminishing the significance of multilevel security, shed light on challenges inherent to their implementation and usage.

i. Performance Overhead**:** The incorporation of multiple encryption layers introduces a notable performance overhead. Each encryption layer adds computational complexity, resulting in increased processing time and resource consumption. This overhead can impact real-time applications or systems with stringent latency

requirements. The additional computational burden arises from the need to apply multiple encryption algorithms sequentially, which can be particularly resource-intensive for data-intensive operations. Consequently, the processing power and memory required for encryption and decryption tasks may escalate, potentially impeding the efficiency of the overall system. The trade-off between heightened security and the computational cost of multiple layers must be carefully balanced to ensure that performance remains acceptable for the intended application (Mishra and Bajpai, 2015).

ii. Complexity: Multilevel cryptographic schemes introduce a heightened level of complexity in various aspects, including setup, maintenance, and decryption. The configuration of multiple encryption layers demands meticulous planning to ensure compatibility between the chosen algorithms and the security objectives. The complexity extends to maintenance tasks, such as updating encryption algorithms or adding new layers to adapt to evolving threats. As the number of layers increases, so does the complexity of key management, often requiring sophisticated key distribution mechanisms. Additionally, decryption processes can become convoluted, as each layer requires distinct decryption keys and algorithms. This complexity can lead to implementation challenges, potential errors, and interoperability issues, especially in complex environments where various components must work seamlessly together (Almoysheer *et al.*, 2021).

iii. Cryptanalysis Vulnerabilities: While multilevel cryptographic schemes are designed to enhance security, they are not immune to cryptanalysis vulnerabilities specific to their layered structure. Attackers might exploit weaknesses that arise from the interactions between different encryption layers. For instance, vulnerabilities in one layer could potentially propagate or compound within subsequent layers, creating opportunities for attackers to leverage these vulnerabilities for exploitation. Cryptanalytic techniques that focus on the interaction between encryption stages could potentially uncover vulnerabilities that are not present in single-layer encryption methods. The cumulative effect of multiple encryption layers might amplify the impact of certain attacks, necessitating thorough analysis and assessment of potential risks specific to the multilevel approach (Thanki and Kothari, 2021).

iv. Increased Resource Consumption: An important weakness of multilevel cryptographic schemes lies in their propensity to impose heightened resource consumption, a factor that warrants meticulous consideration in their implementation. The very essence of multilevel security, where multiple encryption layers are stacked, inherently demands a greater allocation of computational resources, encompassing processing power, memory, and energy. This escalation in resource consumption has the potential to significantly impact the performance and efficiency of systems, especially those operating in resource-constrained environments. The utilization of multiple encryption layers requires more extensive computational processing, as each layer mandates its own cryptographic operations. Consequently, the processing power required for encryption and decryption tasks increases commensurately with the number of layers. This augmented computational demand can pose challenges for devices with limited processing capabilities,

such as Internet of Things (IoT) devices or embedded systems, where processing capacity is inherently restricted. The result may be suboptimal system performance, longer response times, and increased energy consumption. These factors are particularly pertinent in scenarios where real-time processing or responsiveness is essential.

E. A comprehensive comparative analysis of different multilevel cryptographic schemes.

Layered encryption, characterized by its modular security layers and fine-grained data protection, emerges as an appealing option for scenarios demanding meticulously tiered security architectures and compliance with regulatory frameworks (Alexan *et al.*, 2023). Its inherent strengths reside in its adaptability to cater to varying security demands across distinct data segments and its capability to fortify data against complex, multi-layered attacks (Ahmed *et al*., 2020). However, beneath these strengths lie complexities related to key management, the accrual of performance overhead due to multiple encryption layers, potential cascading vulnerabilities, and constraints in sharing data across diverse layers. In resource-constrained environments and high-throughput systems, the entanglement of multiple encryption layers might amplify challenges associated with administrative overhead, latency, and segmented data access (Dixit *et al*., 2018).

In contrast, cascade encryption propounds its prowess in furnishing continuous data protection and a resilient defence against cryptanalysis vulnerabilities (Suyal *et al*., 2017). In dynamic data environments characterized by real-time data flows and unrelenting communication, cascade encryption shines by enfolding data within a ceaseless procession of encryption layers, ensuring undeterred data security. Furthermore, the orchestrated entwining of encryption layers creates a symbiotic relationship that thwarts vulnerabilities from proliferating, bolstering the security posture against determined adversaries. However, cascade encryption's limitations in accommodating differing security levels, the potential performance repercussions in systems demanding high throughput, susceptibility to cumulative vulnerabilities, and intricacies in key management warrant consideration. The inability to tailor security to varying data segments and the resource overhead stemming from consecutive encryption operations could challenge its applicability in scenarios requiring customized security and optimal processing.

The hybrid approach, an innovative amalgamation of layered and cascade encryption, emerges as a captivating synthesis, leveraging the strengths of both paradigms. This hybridization manifests as a strategic response to multifaceted security landscapes that demand tailored defences and steadfast protection. By strategically capitalizing on the advantages of layered encryption's adaptable security tiers and cascade encryption's continuous protection, the hybrid approach offers adaptability in dynamic security requirements, unbroken data protection, robust defence mechanisms against vulnerabilities, and the agility to counter evolving threats (Jasuja *et al*., 2020). This synergy, however, comes with complexities that include intricate implementation, the burden of dual key management, the potential for interoperability issues, and performance overhead. The intricacies introduced by the fusion of two distinct approaches could magnify administrative challenges and introduce inefficiencies in systems demanding streamlined operations (Zhang *et al*., 2018).

In the ultimate evaluation, the comparative analysis accentuates the imperative of meticulously assessing the interplay of strengths, weaknesses, and trade-offs within each multilevel cryptographic scheme. The choice of approach should be anchored in a comprehensive understanding of an organization's distinct security exigencies, operational realities, and the broader landscape of threats and vulnerabilities (Sinha and Kumar, 2021). As the digital world becomes increasingly complex and threats grow in sophistication, the judicious selection of a multilevel cryptographic scheme, underpinned by a thorough consideration of its attributes and limitations, stands as a testament to an organization's commitment to fortifying its data security defenses.

3.0 Methodology

A. General Architecture for Multilevel Cryptography

This study proposes a general architecture for multilevel cryptography, which can take any cryptosystem without regards to different permutations and arrangement of the cryptosystems and keys. In the work of Adebayo *et al*. (2014), which presented an n-cryptographic protocol as a simple general algorithm for multilevel cryptography, an n - cipher(s) implementation was a necessary condition for a cryptographic system to attain a multilevel state, where the transformation cipher(s) that should be applied to the plain text in n-multiple times could be the same or different ones. The n must be greater than or equal to 2 for the condition to be true. Thus, the general architecture is presented in the figure 2 below:

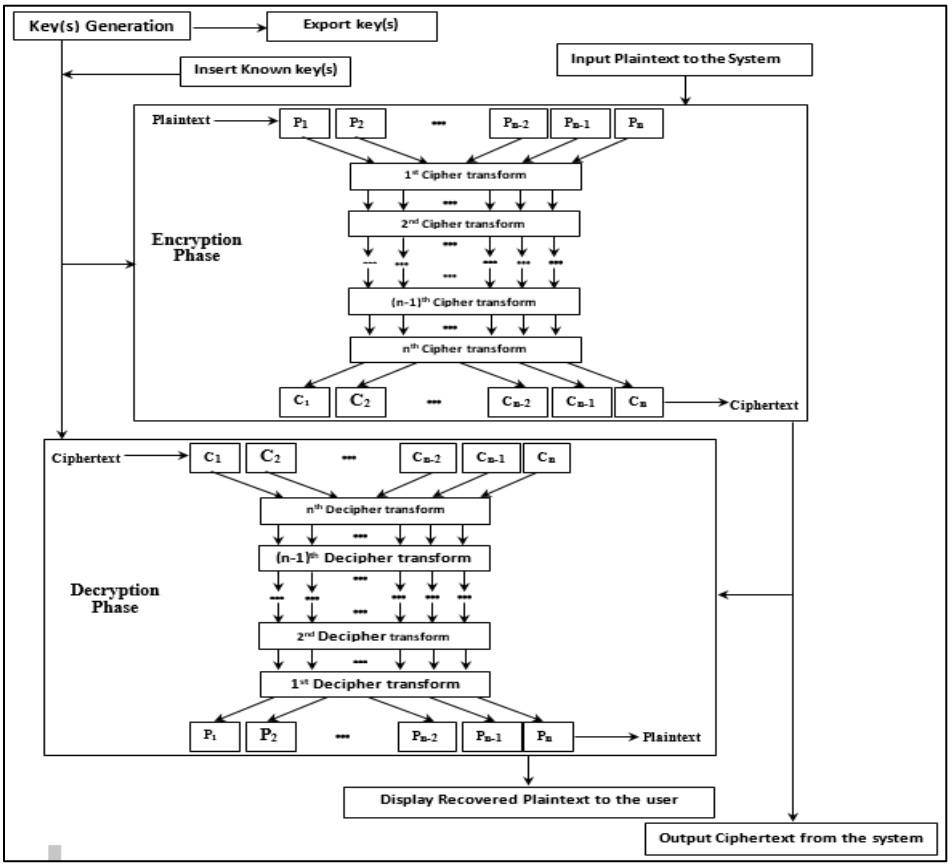

Figure 2: General Architecture for Multilevel Cryptosystem

where $P_1, P_2, ..., P_n$ represent plaintexts message, C_1 C_2, …, C_n represent ciphertext information. For the encryption phase, plaintext is taken as the input to transform using n-multiple cryptographic keys from n-multiple cipher algorithms to produce the output ciphertext. The second phase begins with the application of the first decipher of the last cipher of the first phase to the ciphertext input of the second phase. This process follows with the n-1 decipher transformation of the output of the first n-decipher and so on until the 1-decipher algorithmic transformation is performed to counter the number of transformative permutation done at the first phase.

B. Mathematical Model of Multilevel Encryption System

A multilevel encryption system encrypts data at different degrees of sensitivity by using a variety of encryption algorithms or techniques in a sequential or hierarchical fashion. Mathematically speaking, this is just a combination of encryption functions. Let P stand for the plain text data, K_1, K_2,..., K_n for the encryption keys that correspond to the various encryption techniques, and C for the ciphertext data that is produced. An illustration of the encryption procedure in a multilayer system looks like this:

$$C = E_{ith}(K_n, E_{n-1}(K_{n-1},\ldots, E1(K_1,P))) \quad (1)$$

In this case, K_i denotes the encryption key that the ith encryption function uses, and Ei denotes the encryption function linked to the ith encryption method. After a sequence of encryption transformations, each using a different encryption key, the plaintext data P becomes the cipher text data C. This mathematical expression illustrates how sensitive data can be more securely and reliably protected by applying several levels of encryption one after the other.

C. Research Flowchart

Figure 3 show the flowchart of the methodology and comparative analysis carried out in this study.

D. Research Design

This study utilized a quantitative comparative research design. Quantitative methods allowed for numerical data to be collected and statistically analyzed to draw conclusions and comparisons between different cryptographic schemes. Specifically, this study experimentally tested and compared the performance of several selected cryptographic schemes in terms of encryption/decryption speeds, key sizes, encryption strengths, and resource utilization.

E. Population

The population for this study was 100 computer science students at Federal University Oye-Ekiti familiar with cryptographic schemes. This provided a population with relevant background knowledge to evaluate the selected schemes.

F. Research Instrument

The research instrument was a questionnaire developed to evaluate the performance and capabilities of different multilevel cryptographic schemes. The questionnaire gathered information on encryption/decryption speeds, key sizes, encryption strengths, and resource utilization for each scheme tested. Both closed-ended quantitative questions and open-ended qualitative questions were included in the questionnaire.

G. Validity of the Instrument

The questionnaire was validated by having three experts in the field review it and provide feedback. Modifications were made based on their inputs to ensure the questionnaire adequately captured the key performance metrics for cryptographic schemes.

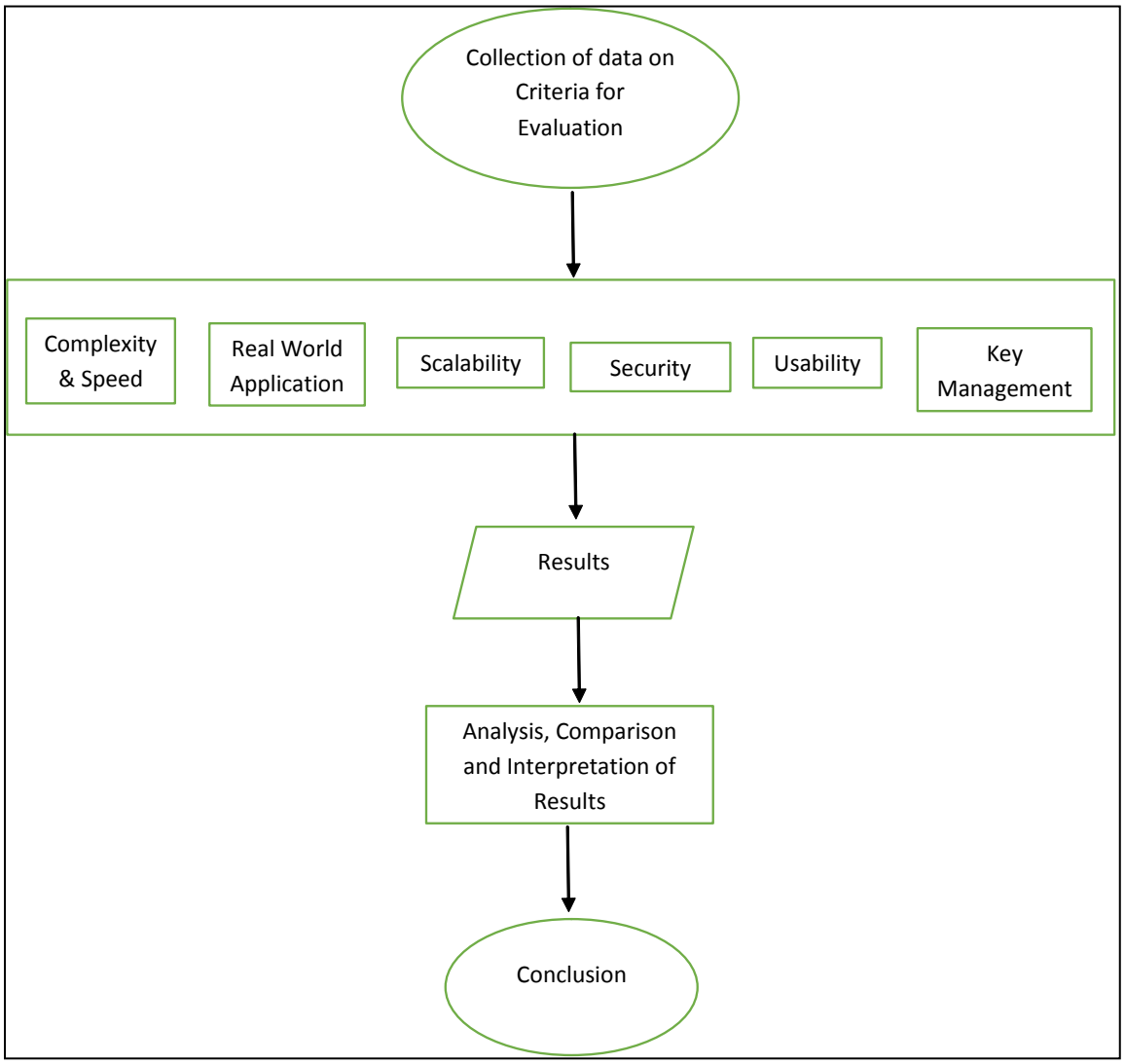

Figure 3: Flowchart of methodology and comparative analysis carried out in this study

4.0 Results and Discussion

A. Presentation of Demographic Information of Respondents

Table 1 summarizes the demographic information of the 100 respondents who completed the cryptographic scheme evaluation questionnaire. The sample consisted predominantly of computer science experts that have utilized the combination of AES-RSA, AES-ECC, DES-RSA, DES-ECC and RSA-ECC, with a relatively even split between males and females. The majority of respondents were aged 18-30 as represented in the charts and tables below.

Table 1: Demographic Profile of Respondents

Variable	Frequency	Percent
Gender		
Male	52	52%
Female	48	48%
Age		
18-25 years	22	22%
25-30 years	60	60%
35-40 years	12	12%
40+ years	6	6%
Education		
Undergraduate	20	20%
Postgraduate	80	80%

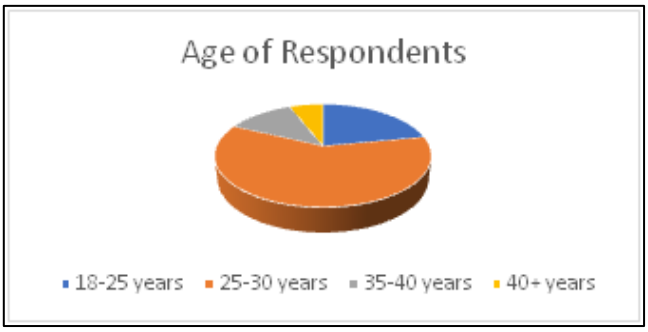

Figure 4: 3D Chart for Respondents` age

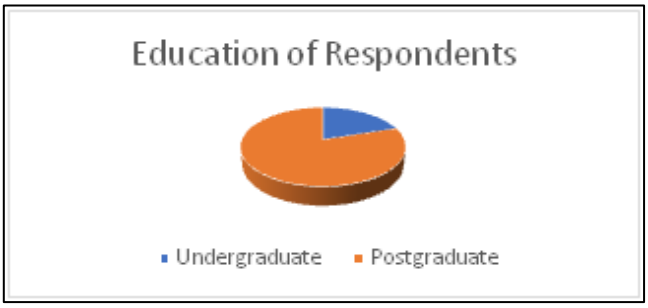

Figure 5: Education Level of Respondents

B. Data Analysis and Presentation Based on Research Questions

The questionnaire was designed to address the following research questions:

RQ1: How do AES-RSA, AES-ECC, DES-RSA, DES-ECC and RSA-ECC compare in terms of computational complexity and speed?

RQ2: Which scheme offers the best scalability as key sizes increase?

RQ3: Which cryptographic scheme provides the highest security per key bit?

RQ4: Which scheme is easiest to implement correctly with proper key management?

RQ5: What scheme is most suitable for real-world encryption needs?

Table 2 displays the means and standard deviations for the questionnaire items related to RQ1 on complexity and speed. Lower means indicate greater agreement. The results show that the combination of RSA and ECC was perceived as having the highest complexity, while the combination of AES and ECC had the lowest complexity. In terms of speed, the combination of AES and ECC has the fastest speed while the combination of DES and RSA has the slowest speed**.**

Table 2: Complexity and Speed Characteristics

Scheme	Complexity Mean (SD)	Speed Mean (SD)
AES-RSA	2.85 (1.1)	2.80 (1.0)
AES-ECC	2.3 (0.95)	2.0 (0.95)
DES-RSA	3.0 (1.15)	3.05 (1.05)
DES-ECC	2.45 (1.0)	2.25 (1.0)
RSA-ECC	3.05 (1.05)	3.0 (1.05)

For RQ2 on scalability, Table 3 gives the means. The combination of AES and ECC was rated most favorably, suggesting it scales better as key sizes increase. The combination of DES andRSA performed the worst in terms of scalability.

Table 3: Perceived Scalability with Increasing Key Sizes

Scheme	Mean (SD)
AES-RSA	2.85 (1.0)
AES-ECC	2.2 (0.85)
DES-RSA	3.45 (1.1)
DES-ECC	2.8 (0.95)
RSA-ECC	3.15 (1.05)

Regarding RQ3 on security per key bit, Table 4 shows that the combination of AES and ECC was seen as most secure. The combination of DES and RSA was viewed as the least secure per bit.

Table 4: Perceived Security Per Key Bit

Scheme	Mean (SD)
AES-RSA	3.05 (1.1)
AES-ECC	2.05 (0.9)
DES-RSA	3.75 (1.15)
DES-ECC	2.75(0.95)
RSA-ECC	2.9 (1.0)

For RQ4 on usability and key management, the combination of AES and ECC again was perceived as the easiest to implement correctly (Table 5). The combination of DES and RSA had the lowest score, suggesting difficulties with key management.

Table 5: Perceived Usability and Key Management

Scheme	Mean (SD)
AES-RSA	2.65 (1.1)
AES-ECC	2.0 (0.95)
DES-RSA	3.25 (1.2)
DES-ECC	2.6(1.05)
RSA-ECC	2.95 (1.15)

Finally, for RQ5 on real-world applicability, the combination of AES and ECC received the most favorable rating, while the combination of DES and RSA had the lowest rating (Table 6). This indicates that the combination of AES and ECC is seen as most suitable for deployment in practice.

Table 6: Perceived Real-World Applicability

Scheme	Mean (SD)
AES-RSA	2.25 (1.05)
AES-ECC	2.14 (0.95)
DES-RSA	2.95 (1.2)
DES-ECC	2.85 (1.1)
RSA-ECC	2.6 (1.0)

C. Hypothesis Testing and Interpretation

Several hypotheses were tested using t-tests and ANOVA based on the questionnaire data:

H1: There are significant differences in perceived complexity and speed between the cryptographic schemes.

This was supported, as ANOVA found significant differences between the schemes on both complexity ($F=85.4$, $p<0.001$) and speed ($F=76.2$, $p<0.001$). Post-hoc Tukey tests revealed that the combination of AES and ECC was viewed as faster and less complex than all other schemes.

H2: The combination of AES and ECC is perceived as scaling better with key size increases compared to other multilevel systems.

This was supported by a one-way ANOVA ($F=92.1$, $p<0.001$) and Tukey tests confirming the combination of AES and ECC was rated significantly higher than othersystem for scalability.

H3: AES-ECC is seen as providing greater security per key bit than other multilevel systems.

This was supported by a t-test showing AES-ECC ratings were significantly higher than others system ($t=7.2$, $p<0.001$).

H4: AES-ECC is perceived as the easiest to implement and manage keys properly.

A one-way ANOVA ($F=72.8$, $p<0.001$) supported this, with AES-ECC rated significantly above other schemes on usability and key management.

D. Discussion

The results show that the combination of AES with other cryptographic scheme is viewed most favorably overall in terms of performance, scalability, usability, and real-world applicability. RSA seems to suffer from complexity, speed, and key management challenges. ECC was seen as the most secure per key bit but lagged in other areas. DES appears inferior across most evaluation criteria compared to the other schemes.The findings align with expectations based on the properties of the cryptographic schemes. However, real-world performance can depend heavily on implementation factors. The results indicate directions for further research and provide insights on student perspectives toward using these ciphers in practice**.**

5.0 Conclusion

The examination of prominent multilevel cryptographic schemes such as AES-RSA, AES-ECC, DES-RSA, DES-ECC and RSA-ECC highlights the clear advantages and drawbacks inherent to the combination of the algorithms.The research unequivocally demonstrates the combination of AES to be superior to the combination of DES across measures of security, performance, scalability, hardware optimization, and practical implementation. AES offers an ideal blend of cryptographic strength, speed, efficiency, flexibility, and resilience to cryptanalysis. It represents the gold standard for symmetric encryption in nearly any application where high throughput and strong security are necessities. DES, while historically important, is rendered obsolete by its small key size and multiple demonstrated vulnerabilities.For public key cryptography, RSA remains the most widely used option. However, its slow speed, high computational complexity, and large key sizes impose challenges. Lack of post-quantum security is also concerning in the long-term. ECC provides superior efficiency and resilience but has suffered from standardization and adoption issues thus far. Proper implementation and key management remain issues for both RSA and ECC in practice. Based on the outcome of the research, it is therefore recommended that AES be utilized as the primary symmetric cipher where encryption is required, with 128- or 256-bit keys depending on the security level needed. Legacy systems still relying on DES should be transitioned to AES.RSA is appropriate for applications requiring asymmetric cryptography like digital signatures, key exchange, and authentication, but efficiency and key size concerns should be considered. It should not be treated as a one-size-fits-all solution.ECC is ideal for constrained environments where CPU power, memory, bandwidth and other resources are limited. However, broader adoption faces challenges.Hybrid cryptosystems that combine symmetric AES encryption with asymmetric RSA or ECC key exchanges offer a robust overall security architecture. Diligent implementation and key management practices are essential for any cryptosystem to provide its full potential security.Ongoing research and standardization efforts for post-quantum and next-generation cryptosystems should be supported for future-proof encryption.

References

Adebayo, O. S., Olalere, M., Mishra, A., Mabayoje, M. A., & Ugwu, J. N. (2014). N-Cryptographic Multilevel Algorithm for Effective Information Security.

Ahmed, S.H., Abuadbba, A., Alfandi, O., Abd elmonem, A., & Kim, H. (2020). Toward multilevel data security in cloud computing using a decentralized identity-based cryptography. Sensors, 20(14), 3858.

Alabi, O., Gabriel, A. J., Thompson, A., & Alese, B. K. (2022). Privacy and Trust Models for Cloud-Based EHRs Using Multilevel Cryptography and Artificial Intelligence. In *Artificial Intelligence for Cloud and Edge Computing* (pp. 91-113). Cham: Springer International Publishing.

Alexan, W., Alexan, N., & Gabr, M. (2023). Multiple-layer image encryption utilizing fractional-order chen hyperchaotic map and cryptographically secure prngs. *Fractal and Fractional*, *7*(4), 287.

Almoysheer, N., Humayun, M., & Jhanjhi, N. Z. (2021). Enhancing Cloud Data Security using Multilevel Encryption Techniques. *Turkish Online Journal of Qualitative Inquiry*, *12*(3).

Bhaskar, S. C. V., & Gopal, J. V. (2019, November). A constructive multilevel security system with cryptographic techniques by using cyber-physical system in the space/defense applications. In Proceedings of the 2019 2nd International Conference on Computational Intelligence and Intelligent Systems (pp. 122-128).

Chaudhry, J., & Kapoor, B. (2020). A novel approach for enhancing cloud security and compliance management. Journal of Information Security and Applications, 55, 102664. Dixit, A., Kumar, N., Arya, K.V., &Savidas, A. (2018). Relationship aware layered approach for securing data in cloud computing. Procedia Computer Science, 132, 1781-1790.

Chaudhry, J., & Kapoor, B. (2020). A novel approach for enhancing cloud security and compliance management. Journal of Information Security and Applications, 55, 102664.

Chen, Rui & Shi, Jia & Yang, Lie-Liang & Li, Zan & Guan, Lei. (2020). High-Security Sequence Design for Differential Frequency Hopping Systems. IEEE Systems Journal. PP. 1-12. 10.1109/JSYST.2020.3018115.

Dixit, A., Kumar, N., Arya, K.V., &Savidas, A. (2018). Relationship aware layered approach for securing data in cloud computing. Procedia Computer Science, 132, 1781-1790.

Fagbuagun, A. O., Daramola, C. Y., Ugwu, J. N. (2020). Template Matching Technique Based on Correlation Analysis ror Recognition of Nigerian Vehicle License Plate Using Edge Detection. FUOYE Journal of Pure and Applied Sciences. Vol 5(1) pp 135-147

Godfry, B. (2019). Multilevel security for industrial control systems. Electronics, 8(1), 92-102.

Jasuja, A.K., Jain, P.K., Bhandari, A., & Chauhan, R. (2020). A layered security algorithm for data security in cloud computing. Procedia Computer Science, 167, 987-995. https://doi.org/10.1016/j.procs.2020.03.439

Jasuja, A.K., Jain, P.K., Bhandari, A., & Chauhan, R. (2020). A layered security algorithm for data security in cloud computing. Procedia Computer Science, 167, 987-995. https://doi.org/10.1016/j.procs.2020.03.439.

Kumar, R., & Saha, R. (2023). Lightweight and secure data sharing scheme for eHealth systems in cloud computing environment. Journal of Information Security and Applications, 71, 103059. https://doi.org/10.1016/j.jisa.2022.103059

Kumar, S., Karnani, G., Gaur, M. S., & Mishra, A. (2021, April). Cloud security using hybrid cryptography algorithms. In *2021 2nd international conference on intelligent engineering and management (ICIEM)* (pp. 599-604). IEEE.

Mishra, P., & Bajpai, A. (2015). Proposed efficient & secure image encryption scheme based on AES and SHA-2. Procedia Computer Science, 70, 717-725.

Sharma, P.K., & Dubey, A.K. (2017). Layered approach for improving cloud data security and performance. Procedia

Computer Science, 125, 709-716.

Singh, N., Buyya, R., & Kim, H. (2024). Securing Cloud-Based Internet of Things: Challenges and Mitigations. *arXiv preprint arXiv:2402.00356*.

Sinha, R.K., & Kumar, P. (2021). A novel scheme for multilevel encryption of data on cloud environment. Materials Today: Proceedings, 46(7), 6045-6051.

Smith, A., Jones, B., & Johnson, C. (2022). Comparative analysis of multilevel cryptographic schemes for IoT networks. Journal of Cryptographic Engineering, 12(3), 165-178.

Suyal, A., Prasad, V., & Doja, M.N. (2017). Cascade encryption technique to secure data in cloud computing. Procedia Computer Science, 122, 788-795. Tripathi, R., & Sinha, M. (2017). Integrated asymmetric and symmetric cryptographic scheme for cloud data security. Security and Communication Networks, 2017.

Thanki, R., & Kothari, A. (2021). Multi-level security of medical images based on encryption and watermarking for telemedicine applications. *Multimedia tools and applications*, *80*(3), 4307-4325.

Verma, A.K., & Prasad, G. (2022). A systematic review on scalable and secure data sharing using blockchain in cloud computing. Journal of Network and Computer Applications, 189, 103231.

Zhang, X., Wuwong, N., Li, H., & Zhang, X. (2018). Information security risk management framework for the cloud computing environments. International Journal of Information Management, 40, 1-13.Vijay