Journal of Theoretical and Applied Information Technology
15th June 2025. Vol.103. No.11
© Little Lion Scientific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A MULTILAYERED SECURITY SCHEME FOR DATA ENCRYPTION AND DECRYPTION FOR STRONGER SECURITY TOWARDS POST-QUANTUM CRYPTOGRAPHY IN CLOUD COMPUTING

[1]DASARI VEERA REDDY,[2]DR.PADMAJA MADUGULA

[1]Research Scholar, Department of Computer Science and Engineering, GST, Gitam Deemed to be University, Visakhapatnam

[2]Asst. Professor, Department of Computer Science and Engineering, GST, Gitam Deemed to be University, Visakhapatnam

Email: vrdasari@gitam.in, pmadugul@gitam.edu

ABSTRACT

Post-quantum cryptography (PQC) is poised to revolutionize data, network, and information system security as quantum computing gains traction. Shor and Grover's methods show how the potential of quantum computing might make cryptographic primitives like RSA and AES susceptible. This suggests that developments in quantum computing are replacing the most advanced conventional encryption methods. Future quantum computers might be far quicker than current ones because of techniques like superposition and entanglement in quantum computing. As such, initiatives are underway to create security solutions that are compliant with PQC. It's important to note that more work will need to be done to construct security primitives compatible with PQC, as the research of these schemes is still in its early phases. The Multilayered Data Encryption Standard (MDES) is one multilayered security technique that addresses this. Because this approach uses many data transformations, data in transit and at rest is exceptionally safe. Encrypting the first layer's data uses the enhanced AES encryption standard. Data availability and integrity are enhanced by slicing and modifying the ciphertext at the second layer using the Optimal Information Dispersal Algorithm (OIDA). The data is converted into an alternate format once slices are created, before the hash value is computed. The data is stored in cloud computing or any other storage system after conversion. Java is the programming language used to construct the specified security solution. An empirical investigation reveals that the proposed technique is highly secure and supports data availability and integrity through a verifiable data loss recovery mechanism. Security research shows the recommended strategy is safer than the most recent methods.

Keywords - *Security, Cryptography, Post Quantum Cryptography, Multi-layered Security Scheme, Data Integrity, Data Availability*

1. INTRODUCTION

Traditional cryptography has been a mainstay of data security for many years, encrypting and safeguarding sensitive data using mathematical techniques. Conventional cryptography has been a foundation of data security for decades, using mathematical principles to encrypt and protect sensitive data. However, the introduction of quantum computing poses a severe threat to current cryptography systems since it can break encryption methods that are now believed to be safe. One of the most significant disadvantages of classical cryptography in the face of quantum computing is that two well-known encryption techniques, RSA and ECC (Elliptic Curve Cryptography), are susceptible to assaults with quantum computers. Quantum computers, which employ quantum bits (qubits) to run computations tenfold quicker than traditional encryption methods, can quickly address the fundamental mathematical problems of conventional cryptography systems.

Researchers are actively working on post-quantum cryptography, also referred to as quantum-resistant cryptography, which intends to produce encryption techniques resistant to quantum attacks to meet the restrictions provided by quantum computing. These cutting-edge cryptographic methods provide data security in the quantum computing era by withstanding quantum computers' processing power. Although classical encryption has proven to be effective in protecting data, its limits in the setting of quantum computing highlight the need to switch to post-quantum cryptographic methods to secure sensitive information in the future [6, 7].

It has been suggested that several post-quantum cryptography primitives might replace existing encryption methods. This group includes multivariate polynomials, hashing, lattice, and code-based cryptosystems. Through mathematical problems that are thought to be complicated even for quantum computers, these primitives seek to provide security in a post-quantum computing environment. Although quantum computing has progressed, by using these novel cryptographic primitives, data security may be guaranteed to remain secure in the post-quantum age. Careful planning and implementation of this modification are required to maintain interaction with current technology and reduce security threats throughout the transition. To protect private information and ensure the ongoing security of digital exchanges and operations, post-quantum encryption will need to be reinforced if the use of quantum technology is ever used [11], [12], and [13].

Previous studies in the post-quantum cryptography domain have primarily focused on either developing secure cryptographic primitives or optimizing specific components like key encapsulation mechanisms or signature schemes. While approaches such as RLWE-based encryption [7], isogeny and lattice-based frameworks [5], and hybrid public key encryption like PQ-HPKE [13] offer strong theoretical resistance to quantum threats, they often lack integrated mechanisms for ensuring data availability and tamper detection in cloud environments. Unlike these isolated solutions, our work is motivated by the need for a unified and layered security model that combines encryption, dispersion, and verification to address real-world scenarios involving cloud storage and transmission. The MDES framework distinguishes itself by employing modified AES with dynamic S-boxes, optimized IDA for resilience, and hashing for integrity validation—all within a cohesive architecture. This layered approach not only strengthens post-quantum resistance but also ensures that data recovery and verification are inherently supported, filling a critical gap left by prior single-layer cryptographic designs.

The things we contributed to this paper are enumerated below. The Multilayered Data Encryption Standard (MDES), a multilayered security method, is suggested in this work. This technique offers robust security for data in transit and at rest with many data transformations. The first data encryption layer uses an enhanced version of the AES standard. The second layer processes the resulting ciphertext using an Optimized Information Dispersal Algorithm (OIDA). This algorithm splits and restructures the data to support data availability and integrity. Before computing a hash value on the data, the data is further changed into another representation following the creation of slices. Finally, the transformed data is stored in any storage infrastructure like the cloud. The proposed security scheme is implemented using the Java programming language. Our empirical study has revealed that the proposed scheme is highly secure besides supporting data integrity and availability with its provable data loss recovery phenomena. According to a security study, the suggested scheme is safer than the most recent ones. The rest of the document is organized as follows: The literature on PQC-compatible methods and other security schemes that improve data security is reviewed in section two. The proposed system and its underlying mechanisms are presented in section three. The results of our experimental study are presented in section four. The significance and limitations of the research are discussed in section five. Finally, section six concludes our work and offers directions for the study's future scope.

2. RELATED WORK

There have been numerous efforts to improve data security in response to the emergence of quantum computing. Grote *et al.* [1] have highlighted the challenge of asymmetric cryptography. They emphasized the need to update processes and protocols for security in anticipation of the impending influence of quantum computers. Dam *et al.* [2] also highlighted the significance of data protection in the digital age, especially given the danger that conventional encryption faces from quantum computing. They mentioned the increasing research on post-quantum cryptography and the standardization initiatives led by NIST. Balamurugan *et al.* [3] discussed the evolution of cryptography from the Caesar cipher to contemporary quantum-resistant systems, focusing on investigating secure algorithms using code-based cryptography. Roy and Kalita [4] noted the risk quantum computing poses to RSA and ECC and highlighted the promise of post-quantum schemes, particularly those based on lattices, in the context of security for limited devices. Borges *et al.* [5] emphasized the essential nature of post-quantum cryptography because RSA and ECC are vulnerable to quantum computing. When evaluating the security and efficacy of post-quantum algorithms, they talked about the preference for isogeny-based systems and RLWE. Chamola and others discussed the promise of quantum computing for exponential data processing on 5G networks and the resulting risk to asymmetric cryptography [6]. Promising solutions such as post-quantum cryptosystems and quantum key distribution were mentioned. Post-quantum cryptography (PQC) aims to withstand quantum attacks while maintaining compatibility with traditional technology, as the researchers Xie and colleagues [7] described. They emphasized the RLWE method while highlighting NIST's standardization of PQC utilizing 26 Round 2 candidates. The Hybrid Universal Network coding Cryptosystem (HUNCC), introduced by Cohen and colleagues [8], demonstrates the possibility for post-quantum security by combining information-theoretic security and public-key cryptography for quick transmission speeds. Kumar and his team [9] emphasized the impending cybersecurity risks. The dangers associated with quantum computing and the necessity of being ready with quantum-immune cryptography. While investigating international initiatives, obstacles, and the viability of quantum-safe algorithms for ICT infrastructure security. Vaishnavi and Pillai [10] contrasted cryptography methods via a SWOT analysis, examining the enhanced capabilities of quantum computing and suggesting improvements to security for post-quantum data transfer.

Gabriel *et al.* [11] claim that the new MQPC framework provides better post-quantum security than RSA and ECC solutions. Cryptography and steganography are crucial for ensuring the security of e-voting systems. Basu *et al.* [12] highlighted the risk of quantum computing to encryption. NIST conducts evaluations of post-quantum algorithms. We compare FPGA and ASIC implementations with NIST PQC candidates. Anastasova *et al.* [13] discussed the balance in public key cryptography and the combination of asymmetric and symmetric approaches in HPKE. They also compared PQ-HPKE versions resistant to quantum computing with RSA, showing minimal overhead. Carames and Lamas [14] emphasized the accountability and openness provided by DLTs and blockchain. Post-quantum cryptosystems enhance blockchain security by addressing concerns related to quantum computing. Roma *et al.* [15] investigated the energy consumption of PQC algorithms, demonstrating high efficiency in lattice-based systems and competitiveness in multivariate techniques.

Pawar and Harkut [16] highlighted the importance of Internet data security when storing personal data across multiple platforms. They compared the efficacy of classical and quantum cryptography in picture encryption. Nejatollahoi *et al.* [17] pointed out the threat posed to standard cryptography by quantum computing and emphasized the need for carefully designed post-quantum lattice-based methods that are agile and diverse across platforms. Campbell [18] examined the vulnerability of ECDSA in well-known blockchains and advocated for the switch to post-quantum lattice-based encryption for cybersecurity. Hekkala *et al.* [19] highlighted the threat posed to data security by quantum computing and emphasized the goal of post-quantum algorithms. They also emphasized integrating post-quantum algorithms into heavily trafficked libraries to increase security. Liu *et al.* [20] mentioned that edge computing requires data encryption. They highlighted the importance of post-quantum cryptography, particularly lattice-based systems, for ensuring long-term security in IoT and edge devices.

In their work, Post-quantum algorithms, such as Goppa codes, were created by Baldi et al. [21] in response to the difficulty in establishing cryptography techniques due to quantum computing. To emphasize the urgent need for processing, Farooq et al. [22], as traditional encryption, is tested by quantum computing. They assessed how well the BIKE and McEliece algorithms performed, offering insightful data for prospective future encryption choices. Ukwuoma *et al.* [23] discussed how encryption hasn't solved the problems with cloud data security, emphasizing the necessity for new paradigms designed for quantum computing. Additionally, they noted that the cloud data security offered by the NTRU and McEliece algorithms is sufficient. Chikouche *et al.* [24] highlighted the need to investigate post-quantum cryptography on mobile devices since traditional public-key methods are vulnerable to quantum computing. They

acknowledged the promise of NTRU Encrypt and NTRU Sign while pointing out security issues with NTRU, Rainbow, and XMSS.
Lone and Naaz suggested using blockchain technology to ensure availability, integrity, and secrecy [26]. They looked at how encryption, digital signatures, and hash functions are used in Bitcoin and Ethereum and stressed how crucial they are to security. The significance of post-quantum cryptography was underscored, along with the continuous endeavors to establish scalable Post Quantum Blockchains. Satrya et al. [27] recommended RSA, NTRU, and SABER to enhance security procedures for safe Internet of Things energy systems. They also showed how a Raspberry Pi running a modified version of NTRU might improve Internet of Things security without requiring additional hardware. They emphasized the need for more study and development to leverage MQTT for IoT fully. Meher and Midhun Chakkaravarthy [28] highlighted the perils of asymmetric keys resulting from quantum computing and the significance of NIST defining post-quantum methods for future security. They proposed a hybrid approach for quantum-safe systems that blends PQC with traditional algorithms. According to Asif [29], post-quantum encryption—like lattice-based cryptography—is essential because quantum computers threaten traditional cryptography. Their survey also examined the usefulness and implementation difficulties of IoT devices. Wang and colleagues [30] emphasized the need for a conventional channel in authentication while highlighting the security of using quantum key distribution (QKD) in combination with quantum computers. They also pointed out post-quantum cryptography (PQC) streamlines authentication processes using a single digital certificate for each user.

Fakhruldeen *et al.* [31] equipped wireless networks with security to fend off quantum attacks. Due to its ability to handle complex tasks, quantum computing has the potential to alter industries like healthcare and fintech significantly. [50]. To enable safe data transfer, new post-quantum cryptosystems are being developed. The effects of quantum computing on DER systems and contemporary cryptography were covered by Ahn et al. [32]. They looked at quantum attack vulnerabilities, defense mechanisms like QKD and PQC, and possible directions for quantum-safe DER network research. Data security was addressed by Karbasi and Shahpasand [33] with Ethereum, a [51] decentralized blockchain with smart contracts. Additionally, they recommended using PAKE, IPFS, smart contracts, blockchain, and PAKE to protect public keys from MITM attacks. Future objectives include creating Ethereum DApps.Their survey analyzed quantum-resistant ABE systems' security, design, and challenges. Carames [35] emphasized the threat of quantum computing to encryption systems, particularly for Internet security. They stressed the need for efficient algorithms for post-quantum Internet of Things devices with limited resources, and researchers are working on creating IoT systems resistant to quantum attacks.

Andrzejczak [36] centered on the NIST standardization process and Post-Quantum Cryptography (PQC). The NIST-selected method Round5 offers KEM and PKE, and there are plans to expand it with error correction codes and non-ring variants, along with investigating area-performance trade-offs in the future. Gaj [37] discussed how Post-Quantum Cryptography, which seeks to protect against quantum attacks using conventional platforms, is affected by quantum computing. Richter *et al.* [38] initiated a contest to find algorithms resistant to quantum errors. The paper examines the finalists of the post-quantum cryptography round three. Hemandez *et al.* [40] discussed the vulnerability of public-key cryptosystems in Internet of Things devices and communications [43]to quantum computers. They looked at the' effectiveness and suitability of post-quantum algorithms for IoT devices operating in resource-constrained environments. Cambou et al. [41] claimed that lattice and code-based cryptography improve security [44] against quantum attacks and use physical unclonable functions (PUFs) for key generation in post-quantum cryptography (PQC). [45] They also mentioned that PUF-based key generation for RAINBOW is being optimized, and PQC throughput is increased via AES hardware acceleration [46] PUFs and high-performance computing benefit from stochastic aspects, which reduce latencies [47]and enhance security. The literature review observed that existing PQC-compatible schemes are still in their early stages [48], and continuous efforts are 49 required to develop genuinely PQC-compatible security primitives.

Despite the growing body of research on post-quantum cryptography (PQC), existing security solutions often lack an integrated, multi-layered mechanism that ensures data confidentiality, integrity, and availability, especially in untrusted public cloud environments. Most studies emphasize individual aspects like encryption or data dispersal but fail to provide a holistic framework that is adaptable for future quantum threats. This gap highlights the need for a secure, scalable, and verifiable data protection model.

Problem Statement: Current cryptographic frameworks are not fully equipped to handle the computational capabilities of quantum attacks while ensuring end-to-end data availability and tamper detection during cloud storage operations.

Research Questions:

How can a security framework be designed to resist both classical and quantum computational attacks while preserving data integrity and availability?

Can a multi-layered encryption mechanism that combines enhanced AES, optimized data dispersal, and hashing improve resistance to evolving security threats?

How does the proposed MDES scheme compare with traditional cryptographic methods in terms of performance, security strength, and operational efficiency?

3. PROPOSED SYSTEM

This section outlines the proposed methodology for enhancing data security, consisting of a security framework, encoding and decoding mechanisms, and underlying algorithms. It discusses a security framework compatible with post-quantum cryptography, incorporating various essential elements to provide comprehensive protection against traditional and potentially quantum computing threats.

3.1 Problem Definition

Security is essential for real-world applications, including government systems. Until 1994, RSA was considered impenetrable and remained secure for four decades until Shor's algorithm's development demonstrated how quantum computers could compromise RSA and other existing methods. However, it takes different amounts of time to break each strategy. In reaction to Shor's discovery, cryptography experts raised the critical length of algorithms to maintain their unbreakability. Additionally, Grover's technique exposed AES's weaknesses when quantum computers were present. AES and RSA are both susceptible to quantum computer attacks.

For instance, Shor's method took 3.58 hours to break the RSA-1024 algorithm, whereas it took 55 hours to break the NIST P-521 algorithm. Grover's algorithm would need 2.6x10^12 years to break AES-128. These findings indicate that existing cryptographic methods become highly vulnerable with the advancement of quantum computers. Although acquiring advanced quantum computers takes time, adversaries have begun using the 'hack now and crack later' strategy, stealing sensitive data and cracking the underlying security when full-fledged quantum computers become available. The potential for quantum computing to surpass conventional computing in speed and power is significant, driven by quantum phenomena like superposition and entanglement. Companies like Microsoft, IBM, and Alphabet are vying for technological leadership in quantum computing, and investment in this subject is growing globally. In light of this, the need for a unique data security technique like post-quantum cryptography (PQC) is paramount, and it is the focus of this research proposal.

3.2 Proposed Data Security Framework

Using post-quantum cryptography to improve data security is essential for several reasons. RSA and ECC, two popular encryption methods, are built on mathematical riddles that quantum computers can quickly solve using techniques like Shor's algorithm. When quantum computers reach their total capacity, they might be able to crack these encryption techniques and jeopardize the protection of confidential information. Many encrypted communications must remain safe for extended periods—sometimes even decades. The goal of post-quantum cryptography is to develop algorithms that are resistant to both potential future quantum attacks and the classical computing techniques that are in use today.

As more sensitive information is transmitted and stored digitally, the risk of interception and decryption increases. Strengthening data security with post-quantum cryptography helps to ensure that confidential data, such as personal information, financial transactions, and government communications, remains protected against evolving threats. In this regard, we have developed a data security framework, shown in Figure 1, which includes mechanisms to enhance security strength for comparison with PQC.

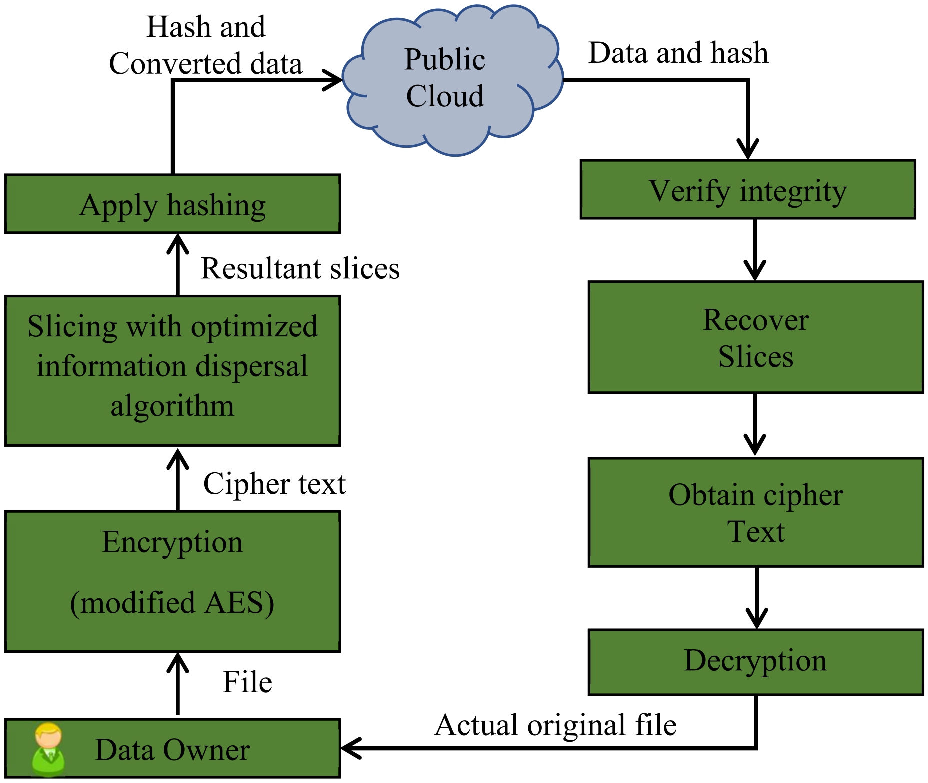

Figure 1: Proposed Framework To Strengthen Data Security And Meet Post-Quantum Threads

The security framework defines a process for protecting data. Initially, an original file undergoes encryption using a modified AES algorithm to produce ciphertext. This ciphertext is then fragmented and processed using an optimized information dispersal algorithm before being hashed. The resulting hashed and converted data and the original hash are then stored on a public cloud. The ciphertext slices are retrieved from the cloud to recover the original file, and their integrity is verified using the stored hash. Finally, the ciphertext is decrypted to restore the original file. The proposed framework includes an encoding process that enhances data security before storing it in the cloud. To get the original data from the cloud, it also has a decoding mechanism that works in reverse of the encoding method.

The proposed MDES framework is inspired by prior research that explored hybrid encryption methods and layered security protocols in the context of quantum-resilient architectures. For instance, Kumar et al. [42] introduced a modified AES algorithm with dynamic S-box generation, which forms the core cryptographic engine in our framework. Similarly, techniques involving information dispersal for enhancing data availability, such as those discussed by Ukwuoma et al. [23] and Fernandez-Carames and Lamas [14], have laid the groundwork for our optimized IDA slicing mechanism. The overall protocol in MDES extends these foundations by offering a structured, end-to-end mechanism that not only encrypts and disperses data, but also verifies integrity before and after cloud storage. This layered model follows the experimental protocol used in previous works—developing the algorithm, simulating data encryption and retrieval, benchmarking performance metrics, and analyzing security strength—making it a validated approach aligned with recent cryptographic practices.

3.3 Encoding Process

An upgraded AES technique encrypts a plain text file as part of the data protection procedure (encoding) shown in Figure 2. After that, it is hashed and sliced using the IDA technique. The original hash and the hashed and transformed data are kept in the cloud. The same key is needed for encryption and decryption since modified AES employs a symmetric encryption technique. The communication parties must disclose this key, which is usually kept confidential. AES encrypts and decrypts data via a sequence of substitution and permutation operations. This arrangement ensures that every plaintext bit affects many ciphertext bits, offering a solid defense against cryptographic assaults.

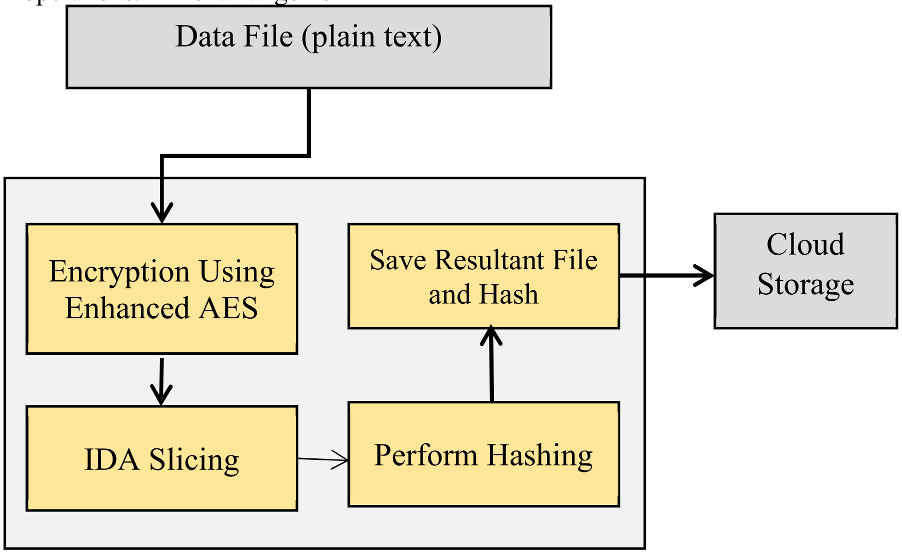

Figure 2: The Modus Operandi Of The Encoding Process

Before storing the data in a cloud architecture, the modified AES is used with specific data alterations, such as IDA slicing, to increase security. To improve cloud storage data security, dependability, and access, communication distribution algorithms, or IDAs, are needed. To enable the data to be distributed over several cloud servers or storage units, IDA first breaks the data into smaller parts. Replication allows for the recovery of the original data from the remaining sections in the unlikely event that some are destroyed or rendered unusable due to device faults or cyberattacks. Through data segmentation into conveniently digestible bits, IDA may improve privacy. The risk of unauthorized access or data breaches exists because no single piece of data exposes the complete set. System resilience is increased by IDA, which distributes data across several servers or locations. Therefore, data loss due to hardware failures, natural disasters, or short-term service interruptions is less likely.IDA may make distributed data, which is dispersed over several nodes, more accessible to retrieve. Customers can still access data from other servers or locations, even if specific nodes experience outages. IDA facilitates the scalability of cloud storage packages. To effectively distribute data across these nodes, IDA may adapt dynamically, and more storage nodes can be added as required. By storing just relevant components across several nodes, IDA might be able to maximize storage utilization. Storage costs may be cheaper overall than with conventional replication-based systems that keep several copies of the data. Processes to verify the integrity of each data component and the quality of the first data reconstruction are frequently used in IDA approaches. This guarantees the completeness and accuracy of the data collected from several sources.

Hashing is necessary for files stored on cloud storage platforms to ensure data accuracy. Hashing functions provide a fixed-size hash result, sometimes called a checksum, based on the contents of a file. This checksum gives an individual depiction of the file contents. It is possible to rapidly identify any changes made to a file by comparing it before and after it is delivered or stored in the cloud and finding its hash value. Hashes are subject to change, regardless of how much material is in the file—hashing results in significantly smaller file sizes most of the time. Computationally efficiently, one may compare hash values without processing or sending the entire file. Hashing values allow for speedy data integrity testing, which is very helpful in cloud storage scenarios where many files are constantly saved and retrieved. One of the primary purposes of hashing is to prevent unwanted file changes. Should someone try to change a file, will the hash values calculated and stored differ? Hashing is another way that file authenticity is verified. A securely communicated hash value may give the receiptor confidence that the file has not been changed during transmission.

3.4 Decoding Process

Safe retrieval processes are crucial in shielding sensitive data stored in the cloud from unwanted users and programs. By preventing unauthorized persons or entities from seeing or intercepting confidential information, these techniques ensure the security and privacy of your data. Secure retrieval techniques also ensure that data recovered from the cloud hasn't been altered or damaged during transfer, purposefully or inadvertently. This comprehensive protection, provided by the cloud, offers a safe way to retrieve altered and stored data, giving you confidence in the safety of your data.

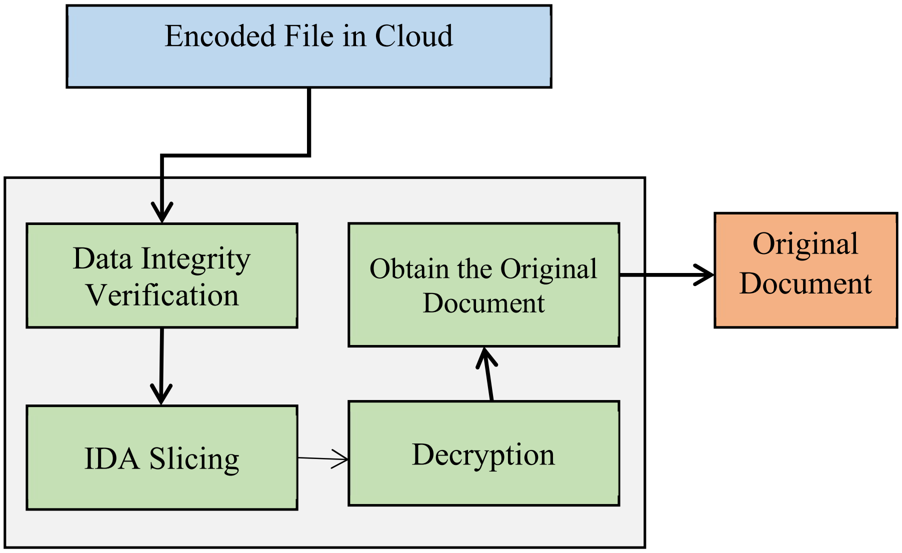

Figure 3: The Modus Operandi Of The Decoding Process

An approach to data recovery and protection based on the cloud is shown in Figure 3. A modified AES algorithm is first used to encrypt a sensitive file. Following IDA's segmentation of the encrypted file into smaller parts, the file's integrity is hashed. These hashed sections are safely kept on a public cloud platform with the original hash. Upon retrieving the encrypted segments from the cloud, the file's integrity is confirmed by comparing it with the saved hash. Afterward, the original data is recovered by decrypting them using the AES technique.

3.5 Modified AES

We have modified the Advanced Encryption Standard (AES) algorithm, drawing inspiration from the work of [42]. During encryption or decryption, a modified Advanced AES dynamically creates replacement boxes (S-boxes) instead of using fixed ones like the original AES algorithm. This approach improves security by adding an element of unpredictability that makes it harder for hackers to crack encryption and decode data.

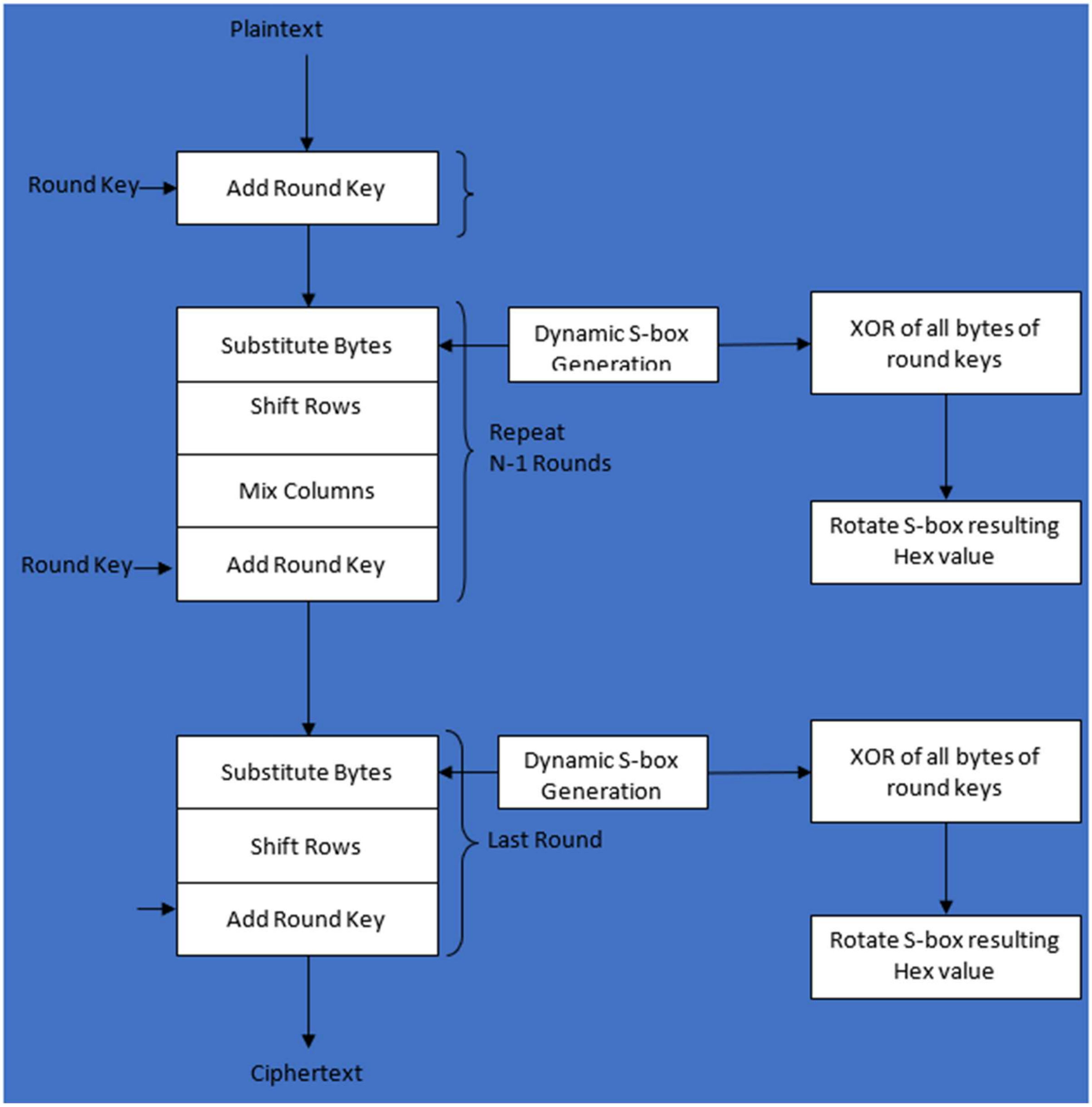

Figure 4: Dynamic S-Box Generation In A Modified AES Algorithm

It is possible to improve the security of the AES algorithm and reduce its susceptibility to well-known attacks like differential and linear cryptanalysis by dynamically generating S-boxes. Through increased complexity and resilience to attacks, dynamic S-box creation decreases the predictability of the encryption process. No predefined S-boxes exist for substitution operations in a modified AES with dynamic S-box building, typically occurring during the Sub Bytes stage. Instead, they are generated by pre-established processes or methods that may use the round number, encryption key, or other data taken from the plaintext or ciphertext. Attackers cannot rely on default S-box attributes because of this unpredictability, making cryptanalysis attempts more challenging. The encryption key usually determines S-box values or settings in dynamic S-box creation. This crucial dependence protects against known-key and brute force attacks by guaranteeing that the key uniquely identifies the S-boxes used during encryption or decryption. Dynamic S-box generation needs to be used very carefully in architecture and validation to ensure that the generated S-boxes do not introduce new vulnerabilities or jeopardize the overall security of the encryption scheme.

Additionally, compared to fixed S-boxes, it could need more processing resources and affect performance. A dynamic S-box can be created to increase the adaptability and flexibility of encryption schemes. Experts in cryptography can experiment with various generation metrics and strategies to customize the S-box creation process to meet particular security needs and resist potential attacks. A robust generation technique impervious to cryptanalytic assaults is essential to the success of the dynamic S-box creation process. Well-designed dynamic S-box generation algorithms must undergo rigorous testing and analysis to guarantee their cryptographic robustness and resistance against attack vectors. Adding a dynamic S-box to a modified AES, which significantly increases the unpredictability and dependency of the encryption and decryption S-boxes, is one popular method to improve algorithm security. Installation and review may offer security advantages, but caution must be used to ensure that the desired outcomes are achieved and that no unanticipated vulnerabilities are introduced.

3.6 Proposed Algorithm

The Multi-layered Data Encryption Standard, or MDES, offers a solid basis for data security in cloud storage. It combines data recovery methods, data distribution (Optimized IDA), integrity checks (Hashing), and encryption (Modified AES) to protect the confidentiality, accessibility, and integrity of stored data. Data loss, corruption, and illegal access are just a few security concerns this technology addresses. Its multi-layered architecture strengthens defense against attacks and guarantees reliable decryption and data recovery for authorized users.

```
Algorithm: Multilayered Data Encryption Standard (MDES)
Input: File (data) of data owner F, secret key k
Output: Encoded file F' and hash of F'

Begin
Encoding
C←ModifiedAES(F, k)
S←OptimizedIDA(C)          //slices generation
H←Hashing(S)
E←Save(S, H)       //encoded output stored in public cloud
Decoding
(H, S)←getFile(id)
Flag←IntegrityVerification(H, original hash)
If flag=true Then
    recoveredSlices←OptimizedIDA(S)
    C←getEncryptedContent(recoveredSlices)
    F←Decrypt(C)
Else
    S←reconstructData(OptimizedIDA, S)
    recoveredSlices←OptimizedIDA(S)
    C←getEncryptedContent(recoveredSlices)
    F←Decrypt(C)
End If
End
```

Algorithm 1: Multilayered Data Encryption Standard (Mdes)

Algorithm 1's objectives include data encryption and secure storage in a public cloud setting. The owner's file (data) and a secret key are the inputs the MDES algorithm needs. It creates a hashed version of the encoded file. In the encoding phase, the secret key encrypts the file using a modified AES algorithm. Slices are produced by analyzing the encrypted material using an enhanced IDA. Following hashing, the slices and hash are stored on the public cloud. The getFile function retrieves the hash (H) and slices (S) from the cloud during decoding. To ensure the integrity of the data, the obtained hash is compared to the original hash.

The slices are located, the encrypted data is eliminated, and the file's original contents are unlocked by decryption after the integrity check. Data is recreated using the upgraded IDA technique if integrity cannot be confirmed. After obtaining the encrypted data, the file is decrypted, the slices are located, and the original contents are exposed. The MDES method facilitates data storage in public clouds by ensuring data security through encryption and integrity checks. An effective IDA for data slicing, hashing for integrity verification, and a modified AES algorithm provides a robust data security architecture. The method's efficiency and security guarantee that the data remains private and safe, even when stored on a public cloud.

4. EXPERIMENTAL RESULTS

In this part, the suggested approach is experimentally analyzed and compared to the current state of security measures. The security strength of the recommended approach is contrasted with well-known approaches like Diffie-Hellman (DH), AES, and RSA. Key exchange TLS, frequently employed in secure communication systems that follow the Diffie-Hellman style, provides several levels of security based on the parameters. The AES algorithm is often considered safe because it can withstand known threats correctly. While quantum computing poses a real risk to the security of RSA, it is still thought to be secure when extensive enough key sizes are used. Results for upload, download, decryption, and encryption timings are also included in this section, along with security assessments.

The results obtained through empirical evaluations directly align with the core objectives of this research. The first objective was to develop a multi-layered data security model capable of withstanding both classical and quantum threats. The proposed MDES framework, by integrating modified AES encryption, IDA slicing, and hashing, meets this goal by ensuring robust confidentiality, data dispersion for availability, and verifiable integrity. The second objective was to validate the effectiveness of the proposed method compared to traditional cryptographic systems. This is clearly demonstrated in Figures 6–10, where the proposed model consistently outperforms RSA, DES, and even standard AES in terms of encryption/decryption time, upload/download efficiency, and overall security strength. These findings support the hypothesis that a hybridized PQC-compatible security approach can deliver both operational efficiency and enhanced protection for data in transit and at rest.

.

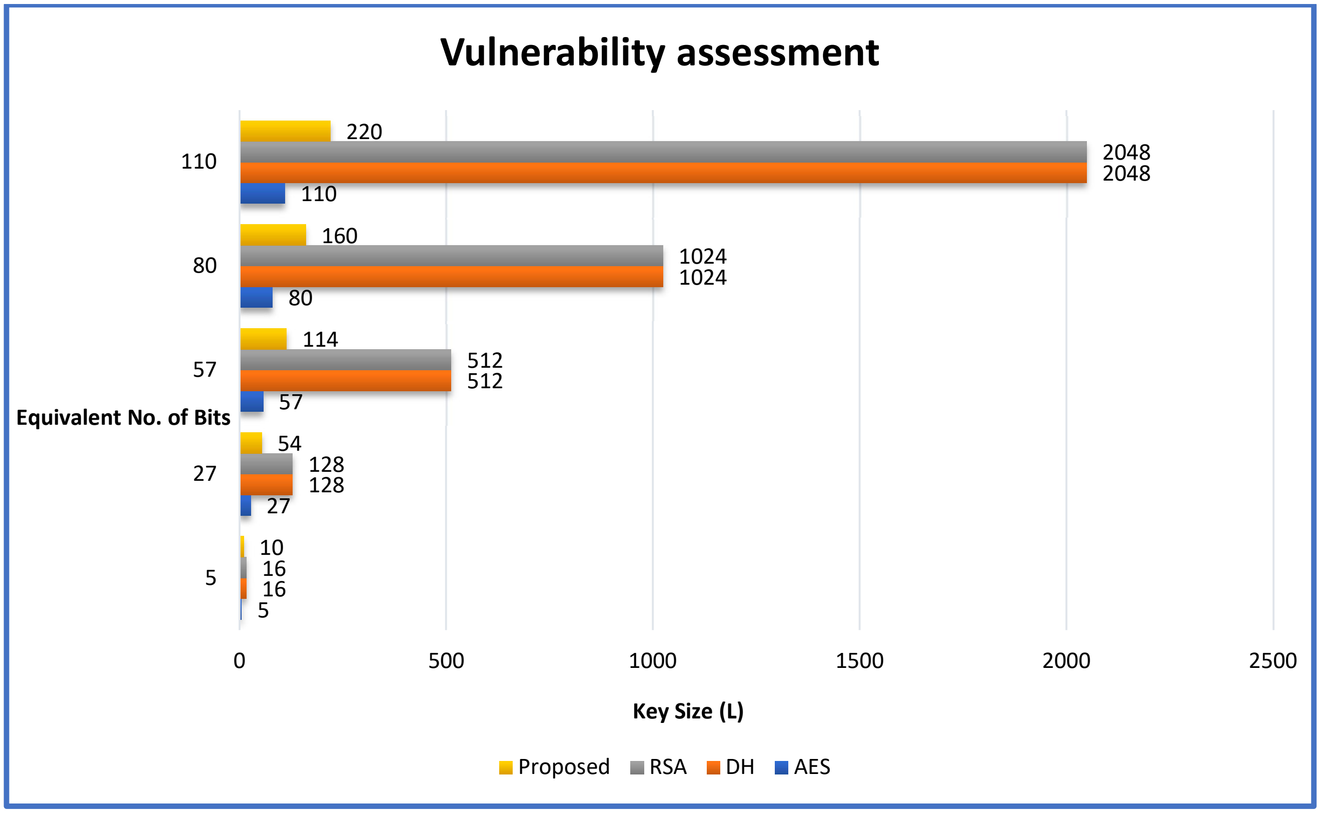

Figure 6: Security Strength Analysis

Figure 6: Security strength analysis. This figure presents a comprehensive comparison of the security strengths and critical sizes of various cryptographic methods. The X-axis displays the corresponding bit count, which spans from 0 to 2500, while the Y-axis denotes the critical size (L)

with specific values: 5, 10, 16, 27, 54, 57, 80, 110, and 220. The bars in the chart represent the security strengths of different algorithms: yellow for the proposed method, gray for RSA (Rivest–Shamir–Adleman), orange for DH (Diffie–Hellman), and blue for AES (Advanced Encryption Standard). The proposed method and MAES achieve the same security levels with significantly smaller key sizes than RSA and DH. For example, to achieve 80 bits of security, RSA and DH need a 1024-bit key, whereas the proposed method and Modified AES require much smaller keys. The most crucial key size for RSA and DH, 2048 bits, corresponds to 114 bits in the suggested technique. This comparison demonstrates how effective AES and the proposed technique offer security with reduced vital sizes, which is crucial for practical implementation.

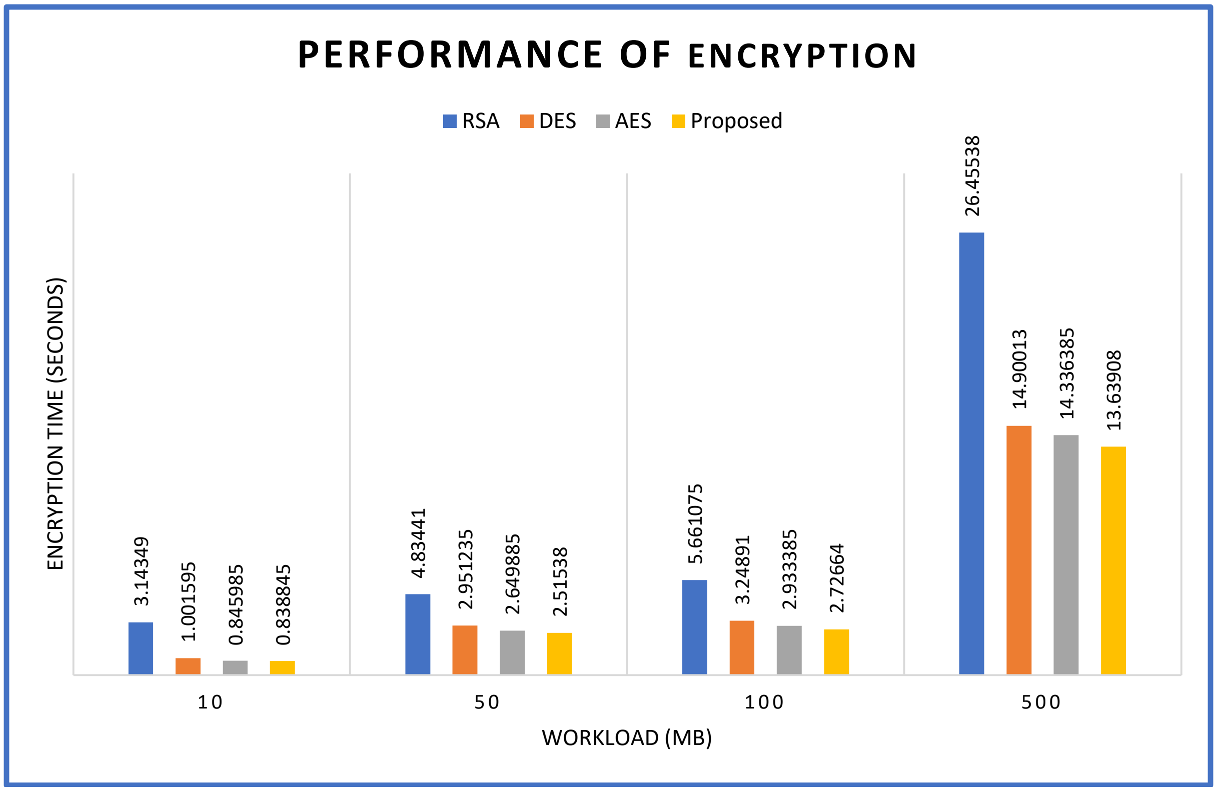

Figure 7: Encryption Time Comparison

Figure 7 compares the encryption times of several cryptographic methods for a range of workloads in megabytes (MB). The X-axis indicates the workload, which has three values: 10 MB, 50 MB, and 100 MB. The Y-axis shows the encryption time in seconds. In the graphic, each technique is denoted by a different colored bar: yellow for the suggested approach, gray for AES (Advanced Encryption Standard), blue for RSA (Rivest–Shamir–Adleman), and orange for DES (Data Encryption Standard). The graph demonstrates that, across all workloads, RSA consistently takes the longest to encrypt data. While RSA is quicker than DES, DES is slower than AES and the suggested technique. AES outperforms RSA and DES in terms of performance, demonstrating faster encryption rates. The proposed approach shows the quickest encryption timings for every workload out of all the methods. Furthermore, all algorithms exhibit increased encryption time with increasing workload; however, RSA shows a more notable increase than the others. The suggested approach is particularly effective and speedy, which makes it perfect for situations requiring rapid data encryption.

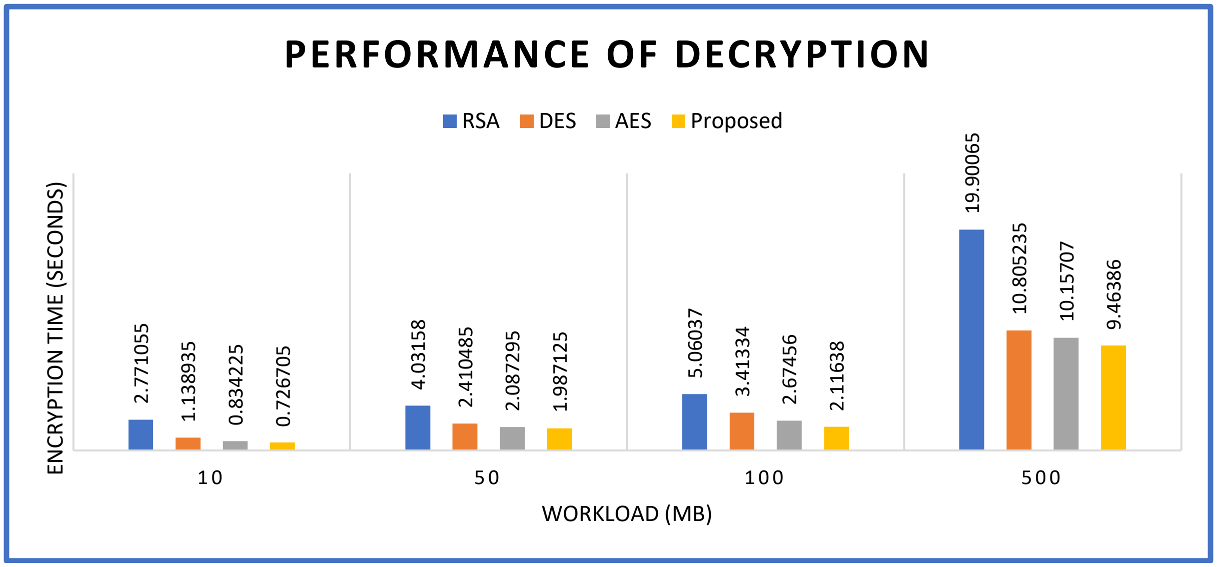

Figure 8: Decryption Time Comparison

The decryption timings of four encryption algorithms—RSA, DES, AES, and a suggested algorithm—across various workloads of 500 MB, 100 MB, 50 MB, and 10 MB are contrasted in Figure 8. For a workload of 10 MB, RSA takes 2.771 seconds, DES takes 1.139 seconds, AES takes 0.834 seconds, and the proposed algorithm takes 0.727 seconds. As the workload increases to 50 MB, RSA's decryption time rises to 4.032 seconds, DES to 2.410 seconds, AES to 2.087 seconds, and the proposed algorithm to 1.987 seconds. At 100 MB, RSA takes 5.606 seconds, DES 3.413 seconds, AES 2.675 seconds, and the proposed algorithm 2.115 seconds. Finally, for a 500 MB workload, RSA's decryption time escalates to 19.991 seconds, DES to 10.805 seconds, AES to 10.157 seconds, and the proposed algorithm to 9.464 seconds. The analysis indicates that the proposed algorithm consistently has the lowest decryption time across all workloads, while RSA exhibits the highest decryption times. DES and AES perform similarly, with DES generally being slightly slower. Additionally, while decryption times increase with workload size for all algorithms, the rate of increase varies among them. Overall, the chart highlights the proposed algorithm's superior efficiency in decryption time performance across the tested workloads.

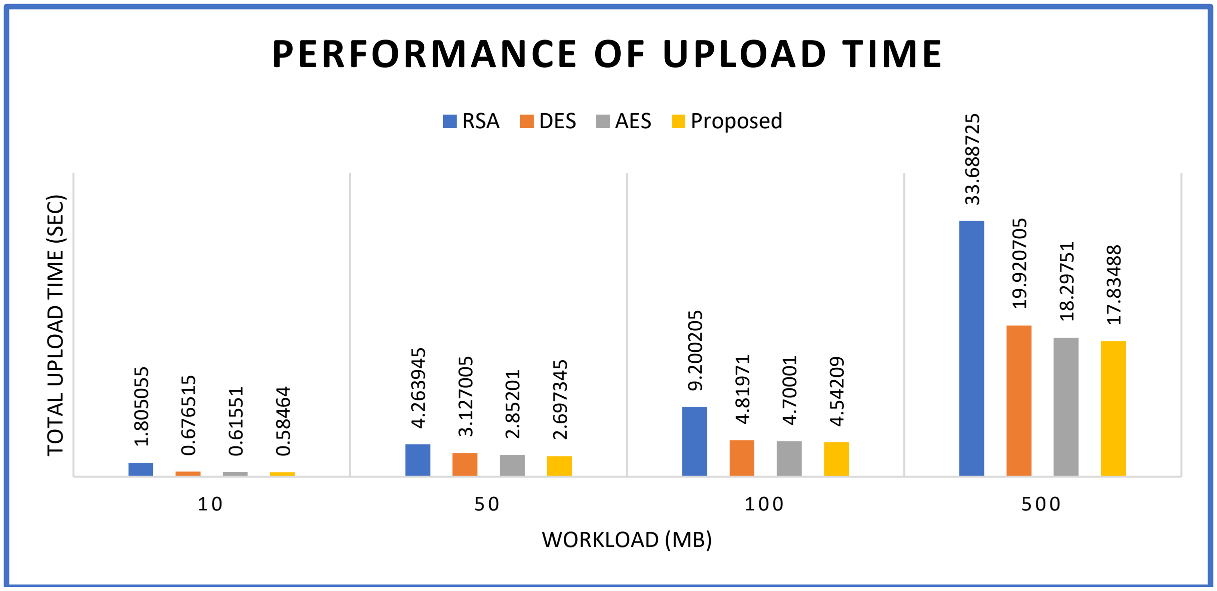

Figure 9: Upload Time Comparison

Figure 9 compares the upload times of four encryption algorithms (RSA, DES, AES, and a proposed algorithm) across three workloads: 10 MB, 50 MB, and 100 MB. For the 10 MB workload, RSA takes 1.805 seconds, DES takes 0.677 seconds, AES takes 0.615 seconds, and the proposed algorithm takes 0.585 seconds. When the workload increases to 50 MB, the upload times also increase: RSA takes 4.264 seconds, DES takes 3.127 seconds, AES takes 2.857 seconds, and the proposed algorithm takes 2.697 seconds. At 100 MB, the upload times increase: RSA takes 9.020 seconds, DES takes 4.820 seconds, AES takes 4.700 seconds, and the proposed algorithm takes 4.542 seconds. Finally, at 500 MB, RSA's upload time is 33.689 seconds, DES's is 19.921 seconds, AES's is 18.298 seconds, and the proposed algorithm's is 17.835 seconds. The analysis indicates that the proposed algorithm consistently exhibits the lowest upload times across all workloads. At the same time, RSA has the highest upload times in every scenario. DES and AES show comparable performance, with DES generally lagging slightly behind AES. Additionally, upload times increase with the workload size for all algorithms, although the rate of increase varies among them. This chart highlights the proposed algorithm's superior efficiency in upload time performance for the tested workloads.

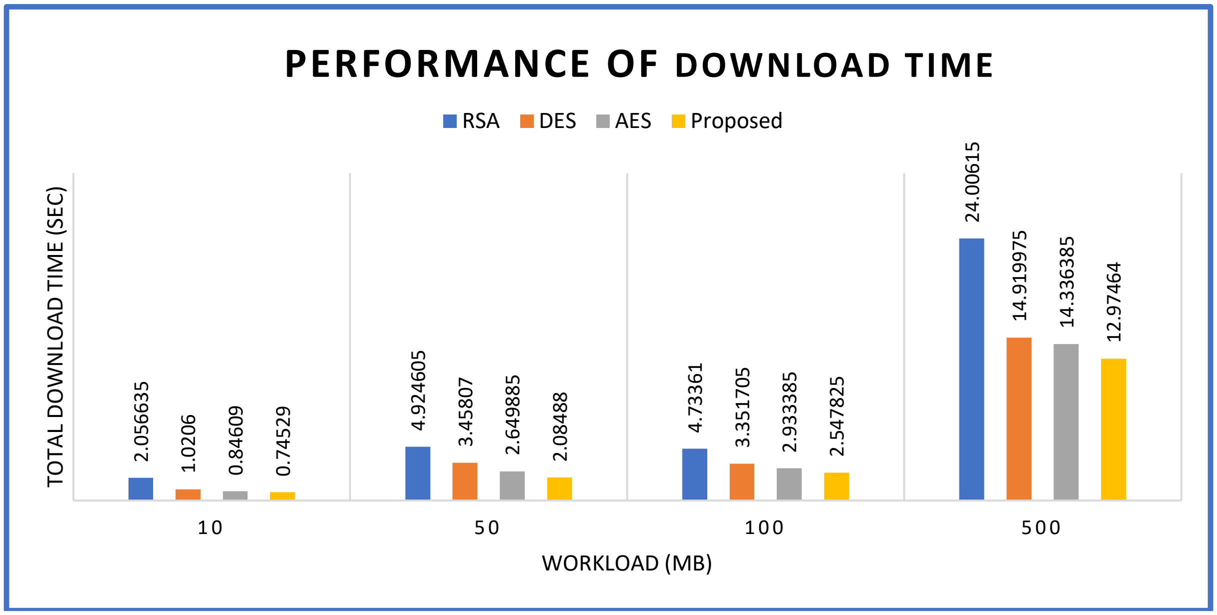

Figure 10: Download Time Comparison

In Figure 10, the download times of four encryption algorithms—RSA, DES, AES, and a proposed algorithm— are contrasted between tasks that total 500, 100, 50, and 10 megabytes. For a 10 MB workload, RSA takes 2.056 seconds, DES takes 1.021 seconds, AES takes 0.846 seconds, and the proposed algorithm takes 0.745 seconds. When the workload increases to 50 MB, download times also increase: RSA takes 4.925 seconds, DES takes 3.458 seconds, AES takes 2.650 seconds, and the proposed algorithm takes 2.085 seconds. For a 100 MB workload, RSA takes 9.734 seconds, DES takes 5.352 seconds, AES takes 2.933 seconds, and the proposed algorithm takes 2.548 seconds. At 500 MB, the download times increase: RSA takes 24.061 seconds, DES takes 14.920 seconds, AES takes 14.337 seconds, and the proposed algorithm takes 12.975 seconds. The data shows that the recommended strategy consistently provides the fastest download times for all workloads. While RSA consistently has the highest. DES and AES show similar performance, with DES typically performing slightly worse than AES. Furthermore, although the growth rate varies, download times rise for all methods as the workload grows. Based on the download time performance for the workloads assessed, the figure shows the overall enhanced efficiency of the recommended strategy.

5. DISCUSSION

The development of post-quantum cryptography was prompted by the possibility that quantum computers would threaten current encryption methods. Popular encryption schemes like RSA and ECC are susceptible to quantum computer cracking because these algorithms are effective at solving certain mathematical problems. For networks and information systems to be protected against this danger, post-quantum cryptography solutions are required. These protocols offer a persistent defense of private data and communications against classical and quantum computer assaults. Updating security procedures, safeguards, and algorithms regularly is also necessary to stay ahead of new threats.

Businesses may be able to strengthen their barriers against potential assaults resulting from developments in quantum technology by implementing post-quantum cryptography strategies and regularly implementing security improvements. The Multilayered Data Encryption Standard (MDES), a special post-quantum encryption technique, provides excellent protection for data at rest and in transit. Several data transformations are employed in this intricate security mechanism. Using an Optimized Information Dispersal Algorithm (OIDA) in the second layer to transmit the ciphertext via data divisions and modifications after the data is encrypted using an updated AES standard in the first layer improves data availability and integrity. After slice creation, the data undergoes two modifications: one into a new representation and another before a hash value is calculated. The data may then be stored using any method, including cloud storage, if necessary. In evaluating the MDES framework against its intended objectives and recent state-of-the-art solutions, several observations emerge. The framework successfully meets its goals of enhancing confidentiality, availability, and integrity through a post-quantum-ready design. It integrates a modified AES variant for stronger encryption, which demonstrates reduced encryption and decryption time compared to traditional RSA and DES. Compared to methods such as PQ-HPKE [13] or lattice-based schemes [5, 17], which focus solely on cryptographic resistance, MDES additionally offers integrity verification and data recovery support—making it a more comprehensive solution. However, unlike some of these specialized cryptosystems that have undergone NIST PQC standardization rounds, MDES remains an integrative framework combining both classical and quantum-resilient components without yet achieving formal certification. Moreover, the performance evaluation, while comprehensive, is based on software simulations and lacks hardware-level validation. Despite these trade-offs, MDES fills a critical gap by unifying encryption, slicing, and verification into a single layered system, which existing standalone cryptosystems often overlook. The shortcomings of the proposed security approach are discussed in Section 5.1.

5.1 Limitations

The suggested data security approach has some drawbacks. Currently, no testing bench uses quantum technology to evaluate the proposed MDES security approach. Another disadvantage is that it is difficult to assess how resilient the proposed approach is to various attacks.

5.2 Open Research Issues

Quantum computing threatens existing cryptographic systems by breaking widely-used schemes like RSA and ECC. While prior studies have developed individual post-quantum solutions focusing on either encryption or key exchange, they often lack a unified, multi-layered approach to ensure data confidentiality, integrity, and availability in cloud environments. This research addresses this gap by proposing a layered security model combining modified AES encryption, optimized information dispersal, and hashing. The core problem lies in securing sensitive data against both classical and quantum threats while maintaining recoverability and tamper resistance. Key research questions include: How can post-quantum resistance be embedded in a holistic framework? Can combined mechanisms enhance security efficiency over existing schemes?

The proposed MDES model fulfills its design goals by outperforming traditional methods like RSA, AES, and DES in encryption/decryption time, upload/download speed, and security strength. It ensures verifiable integrity and supports data recovery via IDA slicing. These outcomes align with the research objectives and demonstrate the practical viability of the proposed framework.

Several directions remain open. The current framework lacks validation in real-world quantum testbeds and secure key exchange mechanisms.

Integration with blockchain and adaptation to IoT environments are potential future enhancements. Lightweight optimization and hardware-level performance testing are also recommended. This work differs from earlier approaches by combining encryption, dispersal, and verification into a single system. Prior works often focused on algorithmic strength alone, without addressing storage resilience or tamper detection. MDES introduces a complete and practical solution by integrating these layers and validating them through performance comparisons.

The research protocol builds on modified AES, dispersal algorithms, and prior quantum-secure frameworks, structured through algorithm development, simulation, benchmarking, and security evaluation. Compared to PQ-HPKE or lattice-based schemes, MDES offers broader protection by addressing availability and integrity alongside encryption.

In conclusion, MDES provides a practical, layered security model that is resistant to quantum threats. It enhances performance, ensures data recoverability, and integrates multiple protection techniques. Future work will involve testbed deployment, integration with secure key exchanges, and adaptation to constrained environments for broader applicability.

6. CONCLUSION AND FUTURE WORK

The Multilayered Data Encryption Standard (MDES), a multilayered security technique, is proposed in this paper. This method, which uses many data transformations, offers high security for data in transit and at rest. An upgraded version of the AES standard is used for the first data encryption layer. An Optimized Information Dispersal Algorithm (OIDA) is used for the resulting ciphertext in the second layer. This algorithm splits and restructures the data to support data availability and integrity. After the generation of slices, the data is transformed further into another representation before a hash value is computed on the data. Finally, the transformed data is stored in any storage infrastructure like the cloud. The proposed security scheme is implemented using Java programming language. Our empirical study has revealed that the proposed scheme is highly secure besides supporting data integrity and availability with its provable data loss recovery phenomena. Security analysis showed that, in terms of security, the suggested system outperforms the most recent ones. We want to assess the proposed security plan in the future inside a certified testbed for PQC. Another direction for the future scope of the research aims to develop a PQC-compatible sharing mechanism that makes data security and key sharing completeness towards robust information systems.

REFERENCES

[1] Grote, Olaf; Ahrens, Andreas; Benavente-Peces, Cesar (2019). A Review of Post-quantum Cryptography and Crypto-agility Strategies, IEEE, pp.115–120. doi:10.1109/IIPHDW.2019.8755433

[2] Duc-Thuan Dam, Thai-Ha Tran, Van-Phuc Hoang and Cong-Kha Pham 1 an. (2023). A Survey of Post-Quantum Cryptography Start of a New Race. MDPI, pp.1-18.

[3] Chithralekha Balamurugan, Kalpana Singh, Ganeshvani Ganesan and Muttuk. (2021). Post-Quantum and Code-Based Cryptography—Some Prospective Research Directions. MDPI, pp.1-30.

[4] Kumar Sekhar Roy and Hemanta Kumar Kalita. (2019). A Survey on Post-Quantum Cryptography for Constrained Devices. International Journal of Applied Engineering Research. 14(11), pp.2608-2615.

[5] Borges, Fabio; Reis, Paulo Ricardo; Pereira, Diogo (2020). A Comparison of Security and its Performance for Key Agreements in Post-Quantum Cryptography. IEEE Access, 8, pp.142413–142422. doi:10.1109/ACCESS.2020.3013250

[6] Vinay Chamola;Alireza Jolfaei;Vaibhav Chanana;Prakhar Parashari;Vikas Hassija; (2021). Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography. Computer Communications, doi:10.1016/j.comcom. 2021.05.019

[7] Xie, Jiafeng; Basu, Kanad; Gaj, Kris; Guin, Ujjwal (2020). Special Session: The Recent Advance in Hardware Implementation of Post-Quantum Cryptography, IEEE, pp.1–10. doi:10.1109/VTS48691.2020.9107585

[8] Alejandro Cohen;Rafael G. L. D'Oliveira;Salman Salamatian;Muriel Medard; (2021). Network Coding-Based Post-Quantum Cryptography . IEEE Journal on Selected Areas in Information

Theory, pp.1–16. doi:10.1109/jsait.2021.3054598

[9] Manish Kumar. (2022). Post-quantum cryptography Algorithm's standardization and performance analysis. Array, pp.1-27.

[10] Anshika Vaishnavi and Samaya Pillai. (2021). Cybersecurity in the Quantum Era-A Study of Perceived Risks in Conventional Cryptography and Discussion on Post Quantum. Journal of Physics: Conference Series, pp.1-12.

[11] Junior Gabriel, Arome; Alese, Boniface Kayode; Adetunmbi, Adebayo Olusola; Adewale, Olumide Sunday; Sarumi, Oluwafemi Abimbola. (2019). Post-Quantum Crystography System for Secure Electronic Voting. Open Computer Science, 9(1), pp.292–298. doi:10.1515/comp-2019-0018

[12] Kanad Basu, Deepraj Soni, Mohammed Nabeel, and Ramesh Karri. (2019). NIST Post-Quantum CryptographyA Hardware Evaluation Study, pp.1-16.

[13] Mila Anastasova, Panos Kampanakis and Jake Massimo. (2022). PQ-HPKE: Post-Quantum Hybrid Public Key Encryption, pp.1-10.

[14] Fernandez-Carames, Tiago M.; Fraga-Lamas, Paula (2020). Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. IEEE Access, pp.1–27. doi:10.1109/ACCESS.2020.2968985

[15] Crystal Andrea Roma;Chi-En Amy Tai;M. Anwar Hasan; (2021). Energy Efficiency Analysis of Post-Quantum Cryptographic Algorithms. IEEE Access, pp.1–23. doi:10.1109/access.2021.3077843

[16] Pawar, Harshad R.; Harkut, Dinesh G. (2018). Classical and Quantum Cryptography for Image Encryption & Decryption, IEEE, pp.1–4. doi:10.1109/RICE.2018.8509035

[17] Nejatollahi, Hamid; Dutt, Nikil; Ray, Sandip; Regazzoni, Francesco; Banerjee, Indranil; Cammarota, Rosario (2019). Post-Quantum Lattice-Based Cryptography Implementations. ACM Computing Surveys, 51(6), pp.1–41. doi:10.1145/3292548

[18] Robert E. Campbell Sr. (2019). Evaluation of Post-Quantum Distributed Ledger Cryptography. The JBBA. 2(1), pp.1-8.

[19] Julius Hekkala, Mari Muurman, Kimmo Halunen and Visa Vallivaara1. (2023). Implementing Post-quantum Cryptography for Developers. SN Computer Science, pp.1-14.

[20] Liu, Zhe; Choo, Kim-Kwang Raymond; Grossschadl, Johann (2018). Securing Edge Devices in the Post-Quantum Internet of Things Using Lattice-Based Cryptography. IEEE Communications Magazine, 56(2), pp.158–162. doi:10.1109/MCOM.2018.1700330

[21] Baldi, Marco; Santini, Paolo; Cancellieri, Giovanni (2017). Post-quantum cryptography based on codes: State of the art and open challenges, IEEE, pp.1–6. doi:10.23919/AEIT.2017.8240549

[22] Sana Farooq, Ayesha Altaf, Faiza Iqbal, Ernesto Bautista Thompson, Debora Libertad Ramírez Vargas, Isabel de la Torre Díez and Imran Ashraf. (2023). Resilience Optimization of Post-Quantum Cryptography Key Encapsulation Algorithms. MDPI, pp.1-24.

[23] Henry Chima Ukwuoma, Gabriel Arome, Aderonke Thompson, and Boniface Kayode Ales. (2022). Post-quantum cryptography-driven security framework for cloud computing. Open Computer Science, p.142–153.

[24] Al-Sharhan, Salah A.; Simintiras, Antonis C.; Dwivedi, Yogesh K.; Janssen, Marijn; Mäntymäki, Matti; Tahat, Luay; Moughrabi, Issam; Ali, Taher M.; Rana, Nripendra P. (2018). Performance Evaluation of Post-quantum Public-Key Cryptography in Smart Mobile Devices, pp.67–80. doi:10.1007/978-3-030-02131-3_9

[25] Agus, Y. M.; Murti, M. A.; Kurniawan, F.; Cahyani, N.D.W.; Satrya, G.B. (2020). An Efficient Implementation of NTRU Encryption in Post-Quantum Internet of Things, IEEE, pp.1–5. doi:10.1109/ict49546.2020.9239560

[26] Auqib Hamid Lone;Roohie Naaz; (2020). Demystifying Cryptography behind Blockchains and a Vision for Post-Quantum Blockchains. 2020 IEEE International Conference for Innovation in Technology (INOCON), pp.1–6. doi:10.1109/inocon50539.2020.9298215

[27] Gandeva Bayu Satrya, Yosafat Marselino Agus and Adel Ben Mnaouer. (2023). A Comparative Study of Post-Quantum Cryptographic Algorithm Implementations for Secure and Efficient Energy Systems Moni. MDPI, pp.1-22.

[28] Kunal Meher and Divya Midhunchakkaravarthy. (2021). NEW APPROACH TO COMBINE SECRET KEYS FOR POST-QUANTUM (PQ) TRANSITION. Indian Journal of Computer Science and Engineering (IJCSE). 12(3), pp.1-5.

[29] Rameez Asif; (2021). Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms, IoT, pp.1-21. doi:10.3390/iot2010005

[30] Liu-Jun Wang, Kai-Yi Zhang, Jia-Yong Wang, Jie Cheng and Yong-Hua. (2021). Experimental authentication of quantum key distribution with post-quantum cryptography. npj, pp.1-7.

[31] Hassan Falah Fakhruldeena, Rana Abbas Al-Kaabi and Feryal Ibrahim Jabbard. (2023). Post-quantum Techniques in Wireless Network Security: An Overview. Malaysian Journal of Fundamental and Applied Sciences. 19, pp.337-344.

[32] Jongmin Ahn, Hee-Yong Kwon, Bohyun Ahn, Kyuchan Park, Taesic Kim. (2022). Toward Quantum Secured Distributed Energy Resources Adoption of Post-Quantum Cryptography (PQC) and Quantum Key Distribu. MDPI, pp.1-20.

[33] Karbasi, Amir Hassani; Shahpasand, Siyamak (2020). A post-quantum end-to-end encryption over smart contract-based blockchain for defeating man-in-the-middle and interception attacks. Peer-to-Peer Networking and Applications, pp.1–19. doi:10.1007/s12083-020-00901-w

[34] Zulianie Binti Jemihin, Soo Fun Tan and Gwo-Chin Chung. (2022). Attribute-Based Encryption in Securing Big Data from Post-Quantum Perspective A Survey. MDPI, pp.1-15.

[35] Tiago M. Fernandez-Carames. (2019). From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things. IEEE INTERNET OF THINGS JOURNAL, pp.1-24.

[36] Andrzejczak, Michał (2019). Annals of Computer Science and Information Systems The Low-Area FPGA Design for the Post-Quantum Cryptography Proposal Round5, 18, pp.213–219. doi:10.15439/2019F230

[37] Gaj, Kris (2018). Challenges and Rewards of Implementing and Benchmarking Post-Quantum Cryptography in Hardware, ACM, pp.359–364. doi:10.1145/3194554.3194615

[38] Maximilian Richter, Magdalena Bertram, Jasper Seidensticker and Alexan. (2022). A Mathematical Perspective on Post-Quantum Cryptography. MDPI, pp.1-33.

[39] Alam, Md Shoaib (2017). Secure M-commerce data using post quantum cryptography, IEEE, pp.649–654. doi:10.1109/ICPCSI.2017.8391793

[40] Jose-Antonio Septien-Hernandez, Magali Arellano-Vazquez and Marco Antonio Con. (2022). A Comparative Study of Post-Quantum Cryptosystems for Internet-of-Things Applications. MDPI, pp.1-18.

[41] Bertrand Cambou, Michael Gowanlock, Bahattin Yildiz, Dina Ghanaimiandoab, Kaitlyn Lee, Stefan Nelson, Christopher Philabaum, Alyssa Stenberg and Jordan Wright. (2021). Post Quantum Cryptographic Keys Generated with Physical Unclonable Functions. Applied Sciences, pp.1-20. doi:10.3390/app11062801

[42] Kumar, P., & Rana, S. B. (2016). Development of modified AES algorithm for data security. Optik - International Journal for Light and Electron Optics, 127(4), 2341–2345. doi:10.1016/j.ijleo.2015.11.188

[43] Srikanth, G., Raghavendran, C.V., Prabhu, M.R., Radha, M., Kumari, N.V.S. & Francis, S.K., 2025. Climate Change Impact on Geographical Region and Healthcare Analysis Using Deep Learning Algorithms. Remote Sensing in Earth Systems Sciences, 130359.

[44] Ravikumar Ch1, Marepalli Radha2, Maragoni Mahendar3, Pinnapureddy Manasa"A comparative analysis for deep-learning-based approaches for image forgery detection International journalof Systematic Innovation https://doi.org/10.6977/IJoSI.202403_8(1).0001

[45] Anitha Patil. (2019). Distributed Programming Frameworks in Cloud Platforms. International Journal of Recent Technology and Engineering (IJRTE). 7(6), pp.611-619.

[46] A. Patil and S. Govindaraj, "An AI-Enabled Framework for MRI-based Data Analytics for Efficient Brain Stroke Detection," 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2023, pp. 1-7, doi: 10.1109/ACCAI58221.2023.10201136.

[47] Sreedhar Bhukya, A Novel Methodology for Secure De duplication of Imagedata in Cloud Computing using Compressive Sensing and Random Pixel Exchanging, Journal of Theoretical and Applied Information Technology (JATIT), Vol.102. No 4, ISSN: 1992-8645 (2024), SCOPUS.

[48] Sreedhar Bhukya, Multiclass Supervised Learning Approach for SAR-COV2 Severity and Scope Prediction: SC2SSP Framework, Volume (12) issue (1), 2025-01-31, SCOPUS.

[49] Ugendhar A.; Illuri B.; Vulapula S.R.; Radha M.; Sukanya K.; Alenezi F.; Althubiti S.A.; Polat K.A Novel Intelligent-Based Intrusion Detection System Approach Using Deep Multilayer Classification Mathematical Problems in Engineering,2022.https://www.scopus.com/sourceid/13082.

[50] Anitha Patil, Dr. Suresh Kumar Govindaraj. (2023). ADL-BSDF: A Deep Learning Framework for Brain Stroke Detection from MRI Scans towards an Automated Clinical Decision Sup. International Journal on Recent and Innovation Trends in Computing and Communication. 11(3), pp.11-23. DOI: https://doi.org/10.17762/ijritcc.v11i3.6195.

[51] P. Sudhakar, D. Prasanna N, S. Bhukya, M. Azhar, G. R Suresh and M. Ajmeera, "Wrapper-based Feature Selection for Enhanced Intrusion Detection Using Random Forest Classification," 2024 International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS), Bengaluru, India, 2024, pp. 1330-1335, doi: 10.1109/ICICNIS64247.2024.10823207.