Journal of Theoretical and Applied Information Technology
31st August 2025. Vol.103. No.16

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

# INTEGRATED ENCRYPTION FRAMEWORK FOR ENHANCED DATA SECURITY IN CLOUD STORAGE

**[1]P HIMA BINDU [2]DR. B. HARICHANDANA [3]DR.BHASKARREDDY T**

[1]Research Scholar S.K. University

[2]Associate Professor Department of CSE SRINIVASA RAMANUJAN INSTITUTE OF TECHNOLOGY.
[3]Professor of Computer Science, S K University

Mails; himabindu5808@gmail.com harichandana4247@gmail.com bhaskarreddy.t@skuniversity.ac.in

**ABSTRACT**

In the contemporary era, there has been a consistent increase in the usage of cloud infrastructure to manage enterprise data. However, there have been security concerns from the data owners' point of view, no matter how good the security of the Cloud Service Provider (CSP) is claimed. Security mechanisms based on cryptography, such as AES, DES, and RSA, have been serving information systems for safeguarding data from adversaries. Although they are effective at protecting data from malicious attacks, future-proof security mechanisms must also consider post-quantum threats. Many of the current studies predicted the possibility of post-quantum security vulnerabilities of existing cryptographic primitives. Motivated by the findings from the literature on the need for novel mechanisms to deal with security of cloud data in post-quantum era, we proposed a novel security framework known as Cloud Data Security Framework (CDSF) that has underlying mechanisms for encoding and decoding that are used to have stronger security when compared with traditional cryptographic primitives such as AES for cloud data encryption and decryption. Moreover, the framework achieves data security, data availability, and data integrity with its mechanisms used for encoding and decoding data. Data owners can use the proposed framework to have secure outsourcing of data and data retrieval even in the post-quantum era. The proposed framework is evaluated with an empirical study using Amazon EC2 cloud infrastructure and found to have better performance over the state-of-the-art cryptographic primitives like AES, DES, and RSA.

**Keywords –***Cloud Computing, Cloud Data Security Framework, Security, Encoding, Decoding*

## 1. INTRODUCTION

Security is an enhanced concern like never before. This is driven by a rise of distributed places, devices, and applications that seamlessly connect modern digital and physical worlds. Data is traditionally protected by mechanisms based on cryptography, which include encryption and decryption. For example, popular symmetric algorithms for data security, both in general and cloud computing, are Advanced Encryption Standard (AES) and Data Encryption Standard (DES). Many researchers aim to develop a hybrid security scheme to enhance security levels; therefore, they modify AES [1]-[3], [8], enhancing AES with a Chaos-based approach for security leveraging. Hybrid cryptography in [8] is implemented with RSA and AES together. Research on improving security has shown up in other areas, including symmetric cryptography, information dispersal, and hashing. In 91215, information dispersal-based security schemes have been explored. This brought some understanding of its importance in terms of the usefulness of the approach for various real-world problems. For example, in [10], an Information Dispersal Algorithm (IDA)- based approach is used for user profiling. IDA provides data integrity and the availability of information.

Yes, many security methods are based on SHA, which is explored in [17]– [24]. It has been applied in other areas like fault detection, image encryption, security improvement, trust-based routing, and data integrity checking, to mention a few. Both lit reviews have a wealth of information concerning the usage of existing encryption algorithms, IDA, and hashing as individual techniques. Besides, many other combinations of hybrid algorithms based on AES and RES have been studied, like [1]- [8]. However, the studies in [29] demonstrate that post-quantum security scenarios merit consideration. In light of these findings, the

current study proposes a security mechanism for encryption/decryption in symmetric key mode based on multiple transformations.

Quantum computing has emerged as a nascent technology with a well-recognized long-term threat to traditional cryptographic systems. Quantum algorithms (for example, Shor's algorithm and Grover's algorithm) can significantly accelerate the time taken to break widely employed public-key and symmetric-key cryptographic schemes by exponentiation, which can present a challenge in securely storing sensitive information. These computational capabilities introduce post-quantum threats: attacks that can violate a problem's confidentiality and validity (for example, the validity of a document or transaction), we'll refer to this as the integrity of the sensitive data, irrespective of the proper implementation of existing cryptographic algorithms.

It requires developing security mechanisms that are secure against a potential attack from quantum adversaries. Those traditional algorithms (AES, RSA, etc.) that do very well against classical attacks, are not quantum-secure by their nature. To overcome this challenge, we propose a Cloud Data Security Framework (CDSF) using a Multi-Layer Hybrid Security Algorithm (ML– HAS), which provides multiple transformations such as enhanced AES, Information Dispersal Algorithm (IDA) and hashing to produce stronger cryptographic primitive in post-quantum era.

Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are well-known symmetric algorithms used to ensure the security of data in general and specifically in the cloud.

Traditional cryptographic systems may be at risk since quantum computing first emerged in recent years. Quantum algorithms — including Shor's algorithm and Grover's algorithm — can break most widely used public-key and symmetric-key encryptions by drastically decreasing the time needed to crack encryption keys. This evolution in computational potency is giving rise to what is termed post-quantum threats, that is, attacks capable of violating the confidentiality and integrity of sensitive information, even where modern cryptographic algorithms are used and properly implemented.

This underlines the immediate requirement to develop and implement security mechanisms that can withstand quantum adversaries. Even though algorithms like AES and RSA resist classical attacks reasonably well, they all lose their built-in security in a post-quantum world. To counter this challenge, our work presents Cloud Data Security Framework (CDSF), which combines a Multi-Layer Hybrid Security Algorithm (ML-HAS) of multiple transforms such as enhanced AES, Information Dispersal Algorithm (IDA), and hashing to form a strong cryptographic primitive that is post-quantum secure.

In this paper, we present a new security framework named Cloud Data Security Framework (CDSF), which embeds different cryptographic mechanisms for securely outsourcing and accessing data in the cloud. ML-HAS is part and parcel of CDSF, where the layered encryption is performed using enhanced AES, fragmentation using Information Dispersal Algorithm (IDA), and Data Integrity verification using SHA-based Hashing. CDSF is a comprehensive approach to providing confidentiality, integrity, and availability of data in hostile environments upon deployment. It is designed for flexible deployment on real-world cloud platforms and is post-quantum secure against the attack of post-quantum with no reliance on vulnerable, single-layer cryptographic primitives. Our contributions are summarized as follows.

In response to the challenge posed by post-quantum security postural, An algorithm called Multi-Layer Hybrid Security Algorithm (ML-HAS) with multiple transformations is developed for a high end security.

The different security layers are demonstrated by building a prototype application, which combines various cryptographic primitive in order to achieve enhanced security.

Data is outsourced to AWS cloud for encryption and outsourced for decryption and the algorithm is evaluated using different size of data where EC2 and S3 resources were harnessed.

The rest of this paper is organized as follows. Literature on various security primitives and respective issues/countermeasures is discussed in Section 2. The preliminaries to the proposed hybrid approach are outlined in Section 3. We present the proposed algorithm details in section 4. Experimental Results Section 5. Section 6 finishes the work performed and paths for future work.

## 2. RELATED WORK

This portion gives an overview on literatures related to modern day data securities. AES algorithm is a symmetric algorithm, using symmetric algorithms may make attacks like brute force, differential, algebraic, and linear attacks [1]. A dynamic S-box and dynamic key generation used a hybrid approach which appears to improve upon AES. MathurBansode [2] proposed text encryption using AES with the dynamics of key generation and use of twelve rounds, and also increased key length of 192 bits. Yang and Chien [3] combined chaotic maps with AES for a new image security method design. The images were found to be secure and effect for security. Darwishet al. In [4], a hybrid algorithm to implement privacy in cloud environment is proposed based on blockchain. Timoty and Santra [5] presented hybrid cryptography algorithm for the security of data and data integrity in cloud.

Salma et al. [6] have also proposed a hybrid-based security scheme for securing data on cloud which is open-ended based on blowfish encryption and AESGORITHM for higher level of security. Case Study-3: Shende and Kulkarni [7] developed a new Hybrid cryptographic primitive by making a combination of RSA and AES. Similarly, Liu et al. Email Security scheme [8] improved RSA and AES better way to funding a security. Mar et al. Using the information dispersal technique, the [9] method is proposed to secure the cloud data. It involves data exchange and secret sharing method for data securities. At least until its eventual discovery was flexible, secure and apparently suitable for giant data. Atoteet al. The algorithm for information dispersal was applied with user profiling to protect it in a distributed atmosphere between one or multiple devices [10].

Nouraet al. To enhance the authentication, availability, integrity and confidentiality, [11] integrated AES and GMAC. They have made the scheme so complex that they hope it will be attacked no more. Designed to use data security in fog computing infrastructure. Qian et al. They focused on Information based Encryption Algorithm lively in [12] to have better access control of information with multiple level facilities. Baldiet al. [13] used probabilistic and parametric model checking to study information dispersal algorithms in terms of confidentiality. [14] Studied for the data protection using techniques similar to fragmentation. While it was improved for parallel processing environments, they found the caveats to be unfavourable. Vidyalakshmiet al. [15] investigated the concept of privacy disposition in the context of information dispersal for privacy preservation. They noted enhanced privacy when it came to controlling visibility of their data.

As part of steganography, Ahmadian and Amirmazlaghani [16] proposed combining the secret sharing of images. [21] is also an example of similar kind of work. Guesmiet al. For security and data integrity, [17] PCR used field model control authentication with image encryption. Kahriet al. For the security of SHA, which is implemented by a fault detection scheme in [18]. For MANETs, Dilli and Reddy [19] proposed a SHA-3 based security solution. (There is a specific algorithm they use called HMAC-SHA3-512.) — Verma and Prajapati [20] proposed Block based bit different technique with modified message digest for security improvement of SHA. It is learned from literature that most of the algorithms using hybrid approach are designed for obtaining better level of security than baseline approaches like RSA and AES. The aforementioned hybrid approaches which rely on RSA lose their lightweight feature on which the importance lies because of the latest types of networks such as Internet of Things (IoT) which produces a lot of data and is consumed in cloud. Furthermore, the studies in [29] have demonstrated the necessity of discussing post-quantum security settings.

## 3. PRELIMINARIES

Details on the AES and IDA used in the proposed security plan is provided in this section.

### 3.1 Advanced Encryption Standard

One of the most widely used encryption techniques is Advanced Encryption Standard (AES), which is the NIST-recommended

standard for data encryption. It supports 128-bit data length and 128/192/256-bit key length. This requires 10/12/14 rounds of computations for key length 128/192/256 bits respectively. Because operations especially AES need AES S-Box (Substitution-Box) that is a matrix of Hex values that are used as lookup table as shown in [25]. S-Box generation is described by: (7) 1.

$$GF(28) = GF(2)[x] / (x^8+x^4+x^3+x+1) \quad (1)$$

The affine transformation is performed that changes the multiplicative inverse by an XOR. AES performs 4 different transformations depicted in Figure 1. In the first step, each byte of the data block is replaced with a corresponding value using the S-Box. Second, according to row position, the state matrix rows are left shifted. The third step: It gets into the multiplication of state matrix columns with fixed matrix columns. Fourth, the round key matrix and the new-state matrix all get XOR work.

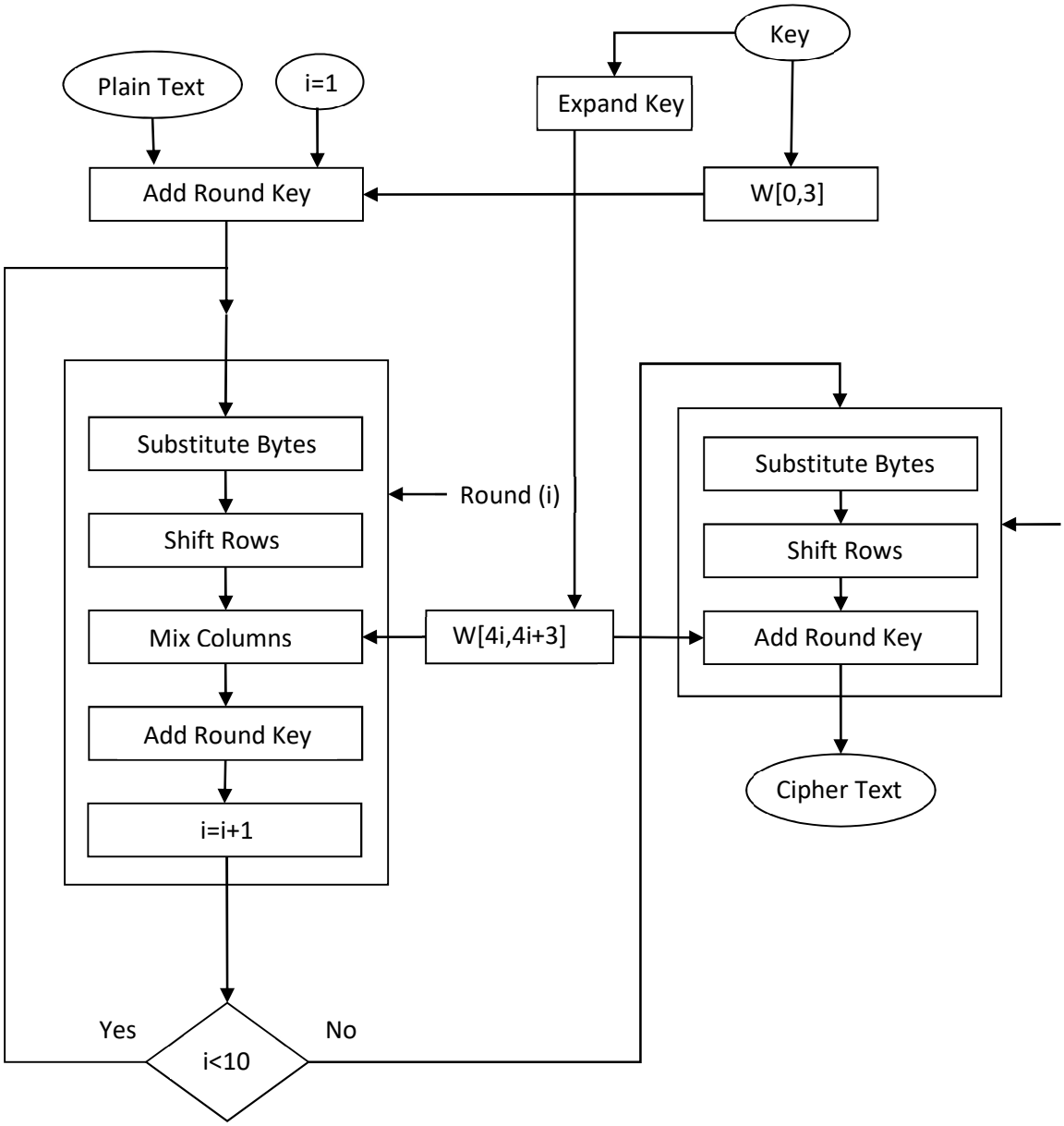

**Figure 1:** Functional overview of AES

This represents some of the limitations of traditional AES. First, the ever-growing nature of cyber-attacks concerns the security experts to think of new schemes as introduced in [26]. To begin with, AES is subject to different kind of attacks, listed in the following: linear, algebraic, and differential [27], [28] and [28]. Third, with the cracking of the algorithm, interception, impersonation and stealing of sensitive information will occur. To mitigate these limitations, enhancements to AES were presented by D'souza and Panchal [1]. These improvements cover dynamic key generation and dynamic S-Box generation. Dynamic keys are generated using the function of time. ItDynamic S-Box: The static S-Box is converted into dynamic S-Box for improved security. Figure 2 depicts the process of dynamic S-Box assignment.

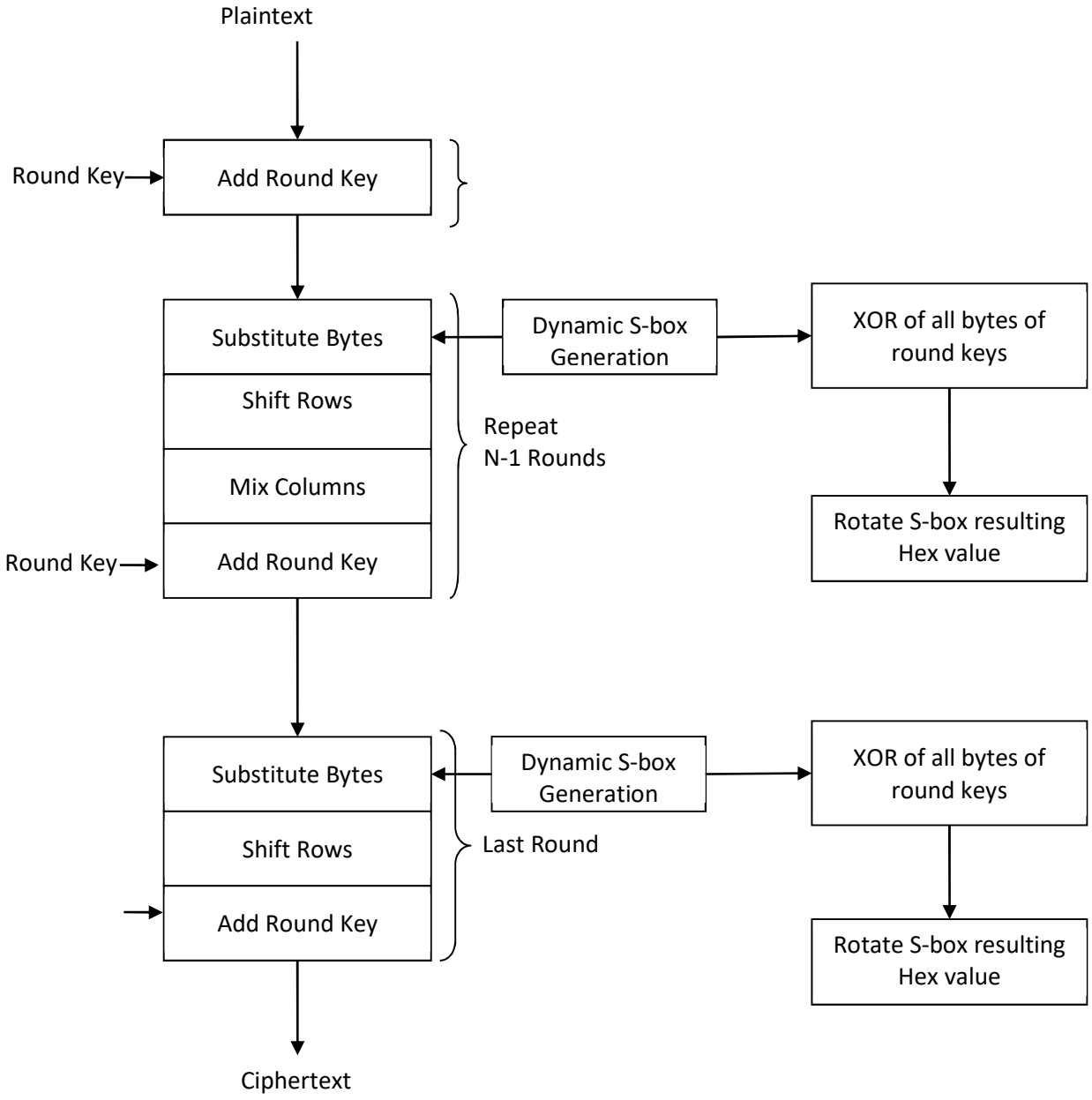


*Figure 2: Flowchart of dynamic S-box generation.*

Journal of Theoretical and Applied Information Technology
31st August 2025. Vol.103. No.16

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

For cryptographic security in the post-quantum era, this improved AES must also be used in conjunction with further changes. In this research, a cryptographic process using hashing and the Information Dispersal Algorithm (IDA).

### 3.2 Information Dispersal Algorithm

It is an algorithm designed for disseminating information efficiently. Let the data in a file be denoted as F = $b_1, b_2, \ldots, b_N$ We assume that the F, and it is expected to lose less than k piece in the face of node failure or communication path problem. The bi may be range of characters (bytes) that must range $0 \leq b_i \leq 255$. In case of data in bytes p=257 is enough, and prime is such that B<p. One chooses a set of n vectors denoted as $Z_p$, i n such a way that there is linear dependency $a_i = \{ a_{i1}, \ldots, a_{im}\} \in Z_p^m, 1 \leq i \leq n$ between m vectors $\{a_1, \ldots, a_n\}$. in that m = m + k satisfies n/m ≤ 1 + ∈ for a specified ∈> o.Length of each sequence is m, and data file F is divided into number of such sequences.

F= $(b_1, \ldots, b_m), (b_{m+1}, \ldots, b_{2m}), \ldots$

denote $S_1 = (b_1, \ldots, b_m)$, etc. For i = 1, ... , n,

$F_i = c_{i1}, c_{i2}, \ldots, c_{iN/m}$

where

$c_{ik} = a_i . S_k = a_{i1} . b_{(k-1)m+1} + \cdots + a_{i.m} . b_{k.m}$ (2)

Let A = $(a_{ij})_{1 \leq i,j \leq m}$ be the m x m matrix whose i-th row is $a_i$. It is readily seen that

$$A.\begin{bmatrix} b_1 \\ . \\ b_m \end{bmatrix} = \begin{bmatrix} c_{11} \\ . \\ c_{m1} \end{bmatrix}$$

and hence

$$\begin{bmatrix} b_1 \\ . \\ b_m \end{bmatrix} = A^{-1}. \begin{bmatrix} c_{11} \\ . \\ c_{m1} \end{bmatrix}$$

Denote the i-th row of $A^{-1}$ by $(\alpha_{i1}, \ldots, \alpha_{im})$, then in general, for 1 ≤ k ≤ N/m,

$b_j = \alpha_{i1}c_{1k} + \ldots + \alpha_{im}c_{mk}$, $1 \leq j \leq N$, (2)

where i = j mod m, k = $\lceil j/m \rceil$ (here we take the residues to be 1, ... , m).

Thus, by operating (2m mod p) on each character of F, F is reconstructed and A is inverted. In handling big files that meet $m^2 \leq |F|$ reconstruction cost drives up the cost of operation. It possible to use additional fields in place of Zp. Such as field E = GF(2^8) has characteristic 2 and 256 elements. In this case, an irreducible polynomial is needed p(x) ∈ $Z_2[x]$ of degree 8 in order to ably set in E.

*Table 1: Notations used in the proposed scheme*

| Change | Description |
|---|---|
| D | Denotes original data |
| $D'$ | Denotes encrypted data |
| $D''$ | Set of slices |
| $D'''$ | Final encoded data |
| $d_i$ | Data file with slices |
| $\delta$, Δ | Denote encryption and decryption respectively |
| Sk | Secret key |

| | |
|---|---|
| $d_i' = H(d_i)$ | Application of hash value |
| ‖ | Operator for concatenation |
| E=$\|D'\|$ | Length of encrypted file |
| P | Denotes number of slices |
| Q | number of symbols/bytes required to reconstruct $D'$ |
| $\ell = \|d_i\|$ | Slice data file length |
| $Y_i = Y_{(i-1)m+1} \ldots\ldots Y_{i.m}$ | Denotes ith blocks of m symbols |
| $\theta$ | Original matrix |
| $d_i = d_{i1}, d_{i2}, \ldots d_{i\ell}$ | File slice |
| C | Cauchy matrix |

The images included in the proposed security plan are displayed in Table 1. We outline the symmetric encryption and decryption security scheme in section 4, along with the encoding and decoding methods.

## 4. ALGORITHM DESIGN

In this, a Multilayer Hybrid security algorithm (ML-HAS) has been proposed to abide with a post-quantum security condition.

### 4.1 Problem Definition

Let file F is owned by data owner outsources towards as a result the data needs to be fully secure. There are chances for cyber-attacks on the data unless it is secured properly before outsourcing the data to cloud. However, symmetric algorithms i.e., the algorithms which are perform the encryption of message, such as AES do have some limitations, as discussed in [22], [23],[24] and [25]. The adversaries of this venerable cryptographic algorithms and their robustness are found to be in the post-quantum cryptographic literature. This paper aims to tackle this issue through multiple iterations of data transformations which is out of scope of the enhanced AES explored in [1].

To address the problem, we fuse improved AES and IDA into the ML-HAS algorithm in a well-planned manner. A symmetric encryption used to provide confidentiality for data is the AES, strengthened to resist classical and quantum cryptanalysis. ORDER also does this by splitting up data into multiple pieces encrypted slices and stored independently. The securityhere is achieved in the sense of fragmentation and in addition to the availability and resilience of data. The original data can still be reconstructed by using threshold-based recovery in the event of loss or tampering of some slices. These mechanisms combined create a resilient hybrid security algorithm capable of withstanding the threats from both classical and post-quantum attacks.

Journal of Theoretical and Applied Information Technology
31st August 2025. Vol.103. No.16

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

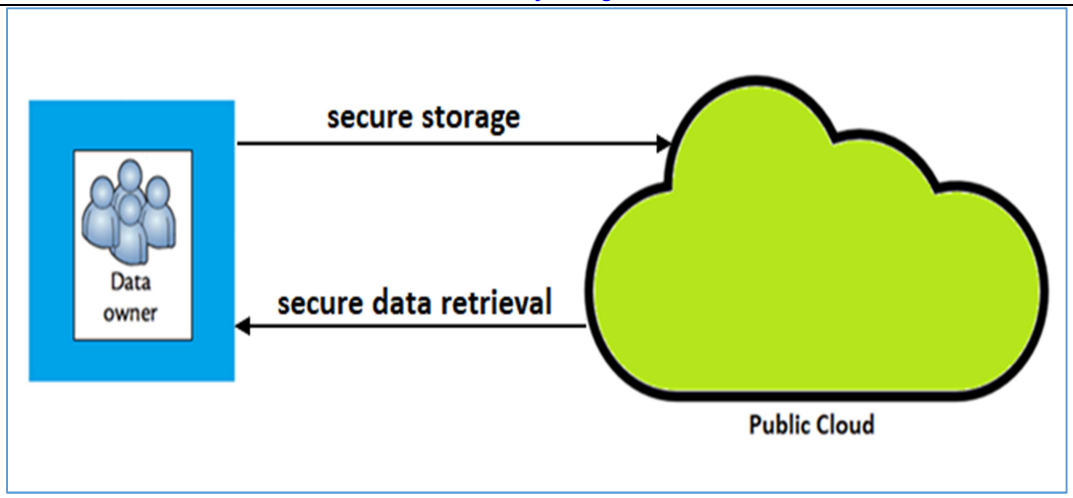


*Figure 3: Conceptual Overview Of Secure Cloud Storage And Retrieval*

In this paper, we concentrate on an issue of ordering server access to the common storage area of (trusted agent protected) and sequence of incoming data packets to support secure storage and retrieval as shown in Fig 3. The proposed Multi-Layer Hybrid Security Algorithm (ML-HAS) algorithm consists of two major operations which are: encoding and decoding. These 3 approaches are detailed in Sections 3.1 and 3.2 respectively.

### 4.2 Encoding Procedure

ML-HAS is purely functioned on two parts related to encoding and decoding processes. Figure 4 demonstrates the encoding process. The data is then transformed many times to make it more secure from cryptographic attacks.

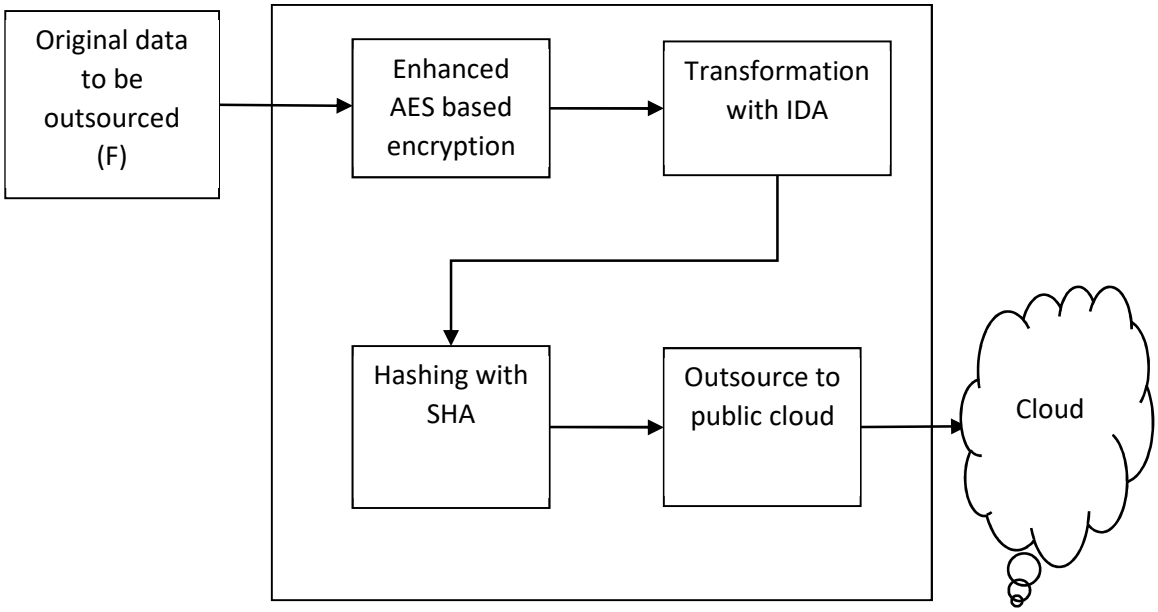


*Figure 4: Overview Of Encoding Process For Secure Outsourcing*

Encryption refers to AES in improved way on the given data. After this, the data is chunked into several slices according to the IDA methodology explained in Section 3.2. Subsequently, each slice is hashed and at the end the encoded info is stored on the public cloud. Try to obtain using IdA and hashing. We look at how IDA can help to recover lost data even if

data slices get lost while hashing can be used to verify the data integrity. Hence data integrity, and data availability.

The algorithm for ML-HAS uses three transformations in succession to encrypt in order to maximize security. Initially, an advanced version of AES is used to encrypt the input file, using a dynamic S-box and dynamic key generation based encryption scheme to improve crptanalysis attack resistence. Second, it applies the Information Dispersal Algorithm (IDA) on the encrypted output that reduces the encrypted data into the number of slices in accordance with some parameters (m,n). This is done so that only a small subset of the slices is needed to recover the original data, thus increasing the availability and failure resistance. Finally, a SHA hash is applied to each slice of the data producing checksums for integrity. These hashes are added into their respective slices and stored in the cloud. This process is inverted for decryption, where file integrity is verified through hashing, IDA reconstructs the encrypted content, and AES is called through a very large and efficient module to decrypt it back to the original file.

The "multiple transformations" in ML-HAS stands for a controlled pipeline of three cryptographic transformations serving to improve different aspects of security. The initial transformation is a stronger AES encryption guarantee of confidentiality based on dynamic keying and substitution logic. The second transformation takes advantage of data fragmentation using Information Dispersal Algorithm (IDA) to achieve availability and fault tolerance by splitting the data into slices such that any subset of the data (above a defined threshold) will be able to reconstruct the original. The final transformation is SHA- based hashing on each data slice, which ensures integrity, as each slice can be verified when retrieving it. This composite increase in layers improves the security model against classical and post quantum adversaries.

**Pseudocode for Encoding Procedure**

**Input:** Data F, Secret key sk, Threshold $(m, n)$
**Output:** Encoded data $F'''$

1. $F' \leftarrow \text{EnhancedAES}(F, sk)$
2. $F'' \leftarrow \text{SliceWithIDA}(F', m, n)$
3. For each $f_i$ in $F''$:
   - $f_i' \leftarrow \text{HashWithSHA}(f_i)$
   - $f_i'' \leftarrow \text{Combine}(f_i, f_i')$
   - Append $f_i''$ to $F'''$

Return $F'''$

*Listing 1: Shows Pseudocode Of Encoding Procedure*

We show the pseudocode that describes the encoding process in Listing 1. Mechanisms like IAM vs. KMS for Encryption, IDA, and 81920 hashing to different transformations push towards a stronger branch of cryptographic certainty.

### 4.3 Decoding Procedure

Once again, the decoding protocols are a subsection of ML-HAS that is the inverse procedure of the encoding protocol. They are used for secure data access from the cloud.

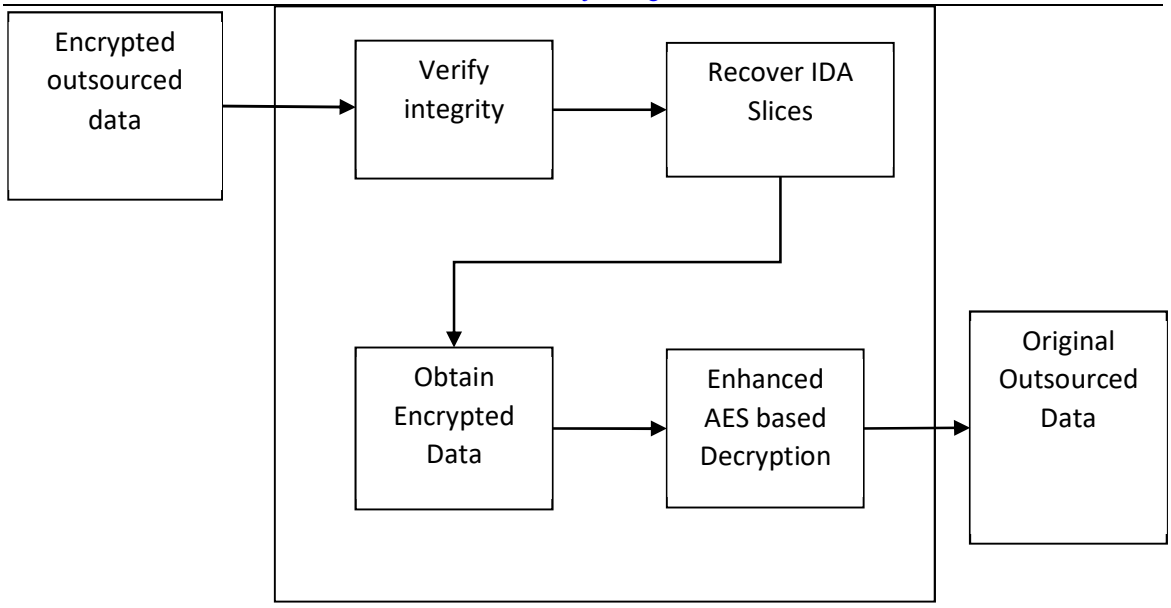


*Figure 5: Decoding Procedure For Secure Data Retrieval*

Decoding is demonstrated as seen in Figure 5. Unlike the encoding process, its mechanisms operate in a reverse order. CDSF does enable an efficient retrieval of the outsourced data even with the advance of quantum computing, thus making sure information would still remain safe. Also, to verify that data slices have not been tampered with on the way to the decoding process, SHA-based hashing integrity checks are performed. In case some slices are missing because of communication failures or attacks, the Information Dispersal Algorithm (IDA) allows recovering the original data by means of a reconstruction that depends on a threshold. The entire encrypted data is then reconstructed and utilizes enhanced AES decryption with dynamic keys to recover the original data. As a result of the multi-layered retrieval process, data confidentiality and data availability are still guaranteed, even when quantum-enabled enemies are involved.

**Pseudocode for Decoding Procedure**

**Input:** Encrypted outsourced data $F'''$, Secret key $sk$, Value $m$
**Output:** Recovered data $F$

1. Initialize $F'$
2. Initialize $F''$
3. Initialize $F'''$
4. For each fragment $f_i$ in $F'''$:
   - If integrity check passes:
     - $f_i \leftarrow Deconcatenate(f_i'')$
     - Append $f_i$ to $F''$
   - Else:
     - Recover data
5. $F' \leftarrow SlicesWithIDA(F'')$
6. $F \leftarrow EnhancedAES(F'$, decrypt mode)
   Return $F$

*Listing 2: Pseudocode For Decoding Procedure*

Listing 2 introduces the pseudocode for the decoding process. It contains the mechanisms on the reverse side of the multiple transformations, resulting in a greater degree of cryptographic security during data retrieval.

## 5. EXPERIMENTAL RESULTS

Journal of Theoretical and Applied Information Technology
31st August 2025. Vol.103. No.16

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

In this section, we report our experimental results and the environment where the empirical study was performed.

### 5.1 Experimental Setup

Storage and performing experiments on Amazon EC2 cloud infrastructure.

### 5.2 Results

Experiments are conducted on the uploading, downloading, encoding, and decoding execution times process with the ML-HAS, and AES, DES, and RSA results compare with others.

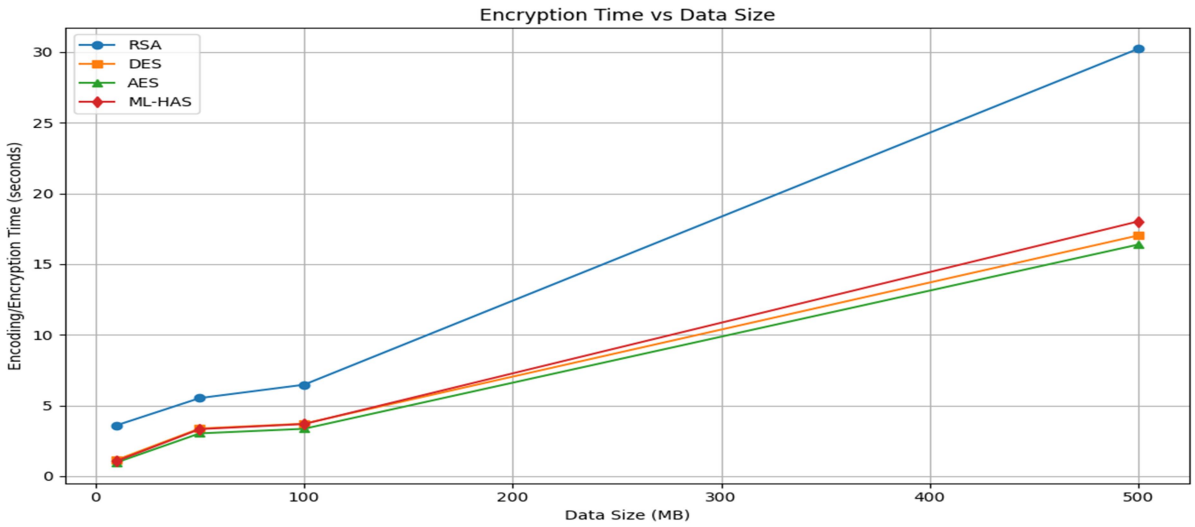


*Figure 6: Encoding/Encryption Time Comparison*

In Figure 6, encoding or encryption time was evaluated for RSA, DES, AES, and ML-HAS across data sizes of 10MB to 500MB. RSA showed the highest encryption time in all scenarios, highlighting its intensive computational requirements due to its asymmetric nature. As the data size increased, RSA's encryption time grew significantly, reaching over 30 seconds for 500MB. In contrast, DES and AES, both symmetric key algorithms, provided faster performance, with AES being slightly more efficient than DES in larger datasets. ML-HAS, the proposed machine learning-based hybrid method, performed nearly as fast as AES, even outperforming DES at certain data sizes. Particularly at 500MB, ML-HAS achieved an encryption time of 18.02 seconds, which is a significant improvement over RSA and comparable to AES. This suggests that ML-HAS offers a well-balanced approach, optimizing speed without compromising the encryption process, making it suitable for secure and time-sensitive data transmissions.

Journal of Theoretical and Applied Information Technology
31st August 2025. Vol.103. No.16

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

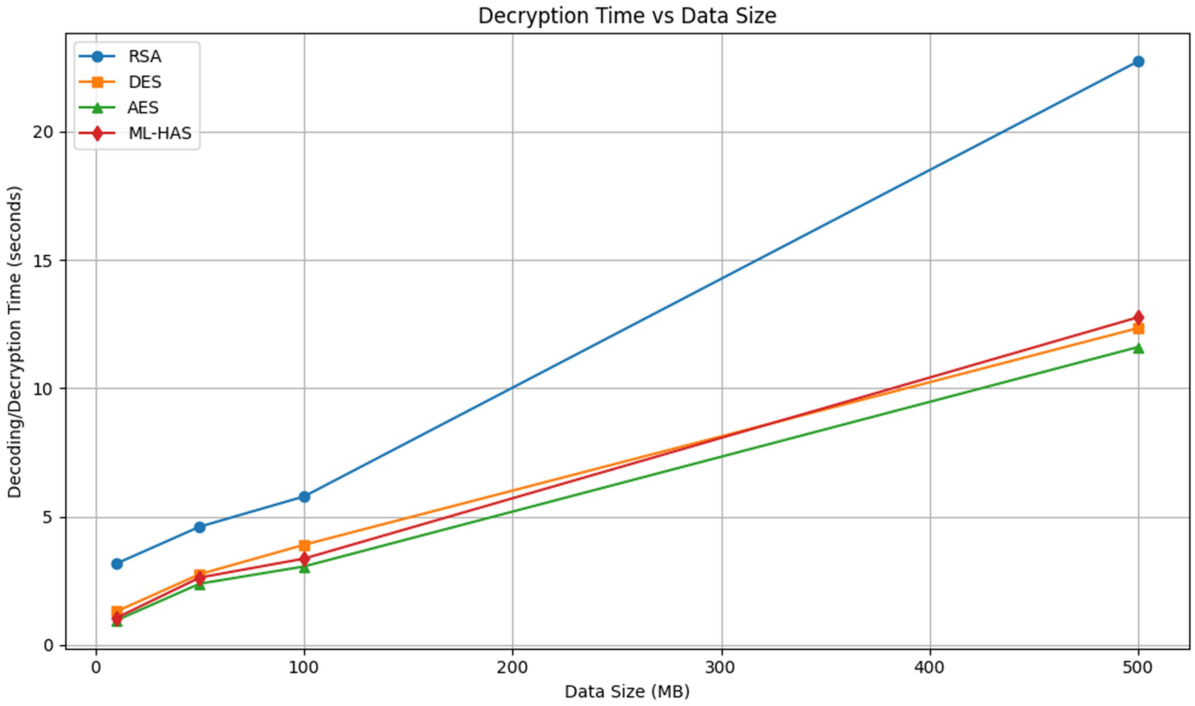


*Figure 7: Decoding/Decryption Time Comparison*

In the above figure 7 when analyzing decryption time, RSA again exhibited the slowest performance, especially as the data size increased, reaching approximately 22.74 seconds for 500MB. This is expected, given RSA's asymmetric encryption structure that requires substantial computational resources. Both DES and AES showed much better results, with AES consistently outperforming DES, particularly at higher data sizes. ML-HAS delivered strong results, closely rivaling AES and surpassing DES in most cases. For example, with 500MB of data, ML-HAS completed decryption in 12.76 seconds—faster than DES and significantly better than RSA. This consistent performance demonstrates ML-HAS's efficiency in handling large-scale decryption tasks. The results show that ML-HAS can maintain fast and reliable decoding speed, making it a viable candidate for real-time or large-volume applications that demand rapid turnaround without sacrificing security. The steady trend across increasing data sizes further validates the robustness of ML-HAS in scalable environments.

Journal of Theoretical and Applied Information Technology
31st August 2025. Vol.103. No.16

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

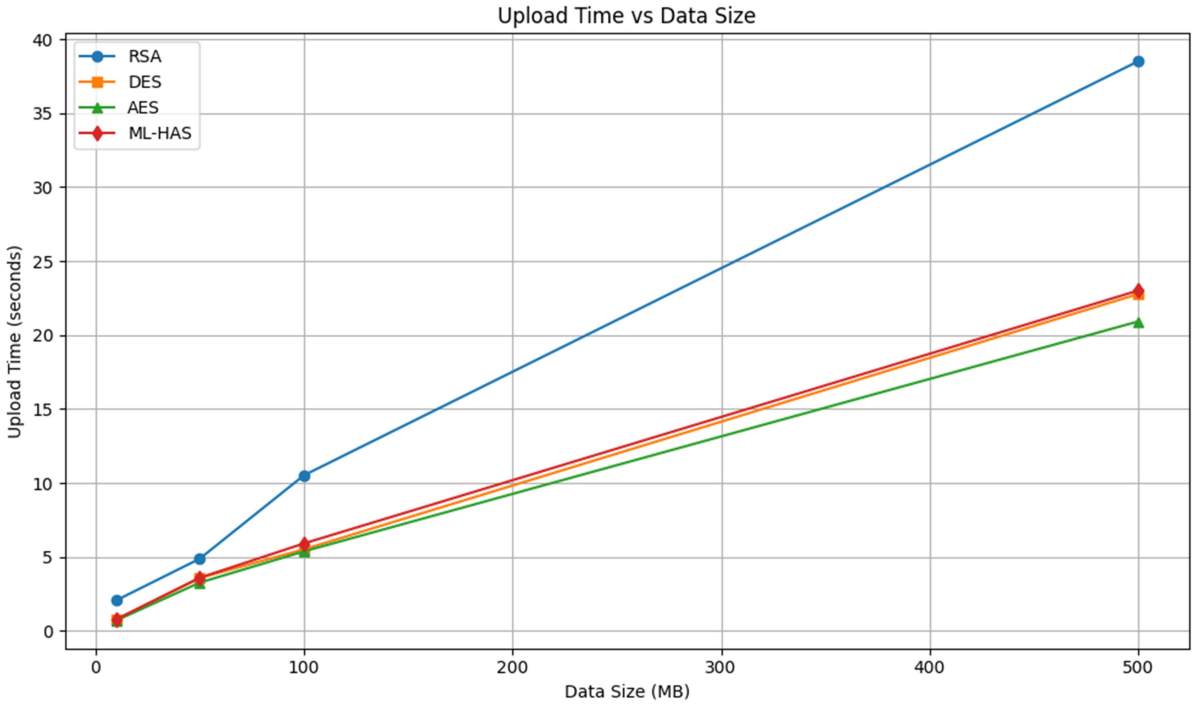


*Figure 8 : Upload Time Comparison*

In the above figure 8 upload time performance reflects how quickly data can be encrypted and transmitted to a remote server. RSA once again lagged behind other methods, especially with larger file sizes, where it took over 38 seconds to upload 500MB—almost double the time of the other algorithms. DES and AES showed better performance, with AES having the slight upper hand due to its more optimized block structure. ML-HAS demonstrated remarkable performance consistency across all data sizes, maintaining upload speeds comparable to AES and even outperforming DES in larger sizes. For instance, for 100MB, ML-HAS had an upload time of 5.91 seconds compared to DES's 5.51 and RSA's 10.51. This trend proves ML-HAS's capacity for handling encrypted data uploads efficiently. Its reliable performance indicates that ML-HAS can serve in secure communication systems, where fast upload speed is crucial, especially in telemedicine, smart surveillance, or other real-time data-driven applications.

Journal of Theoretical and Applied Information Technology
31st August 2025. Vol.103. No.16

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

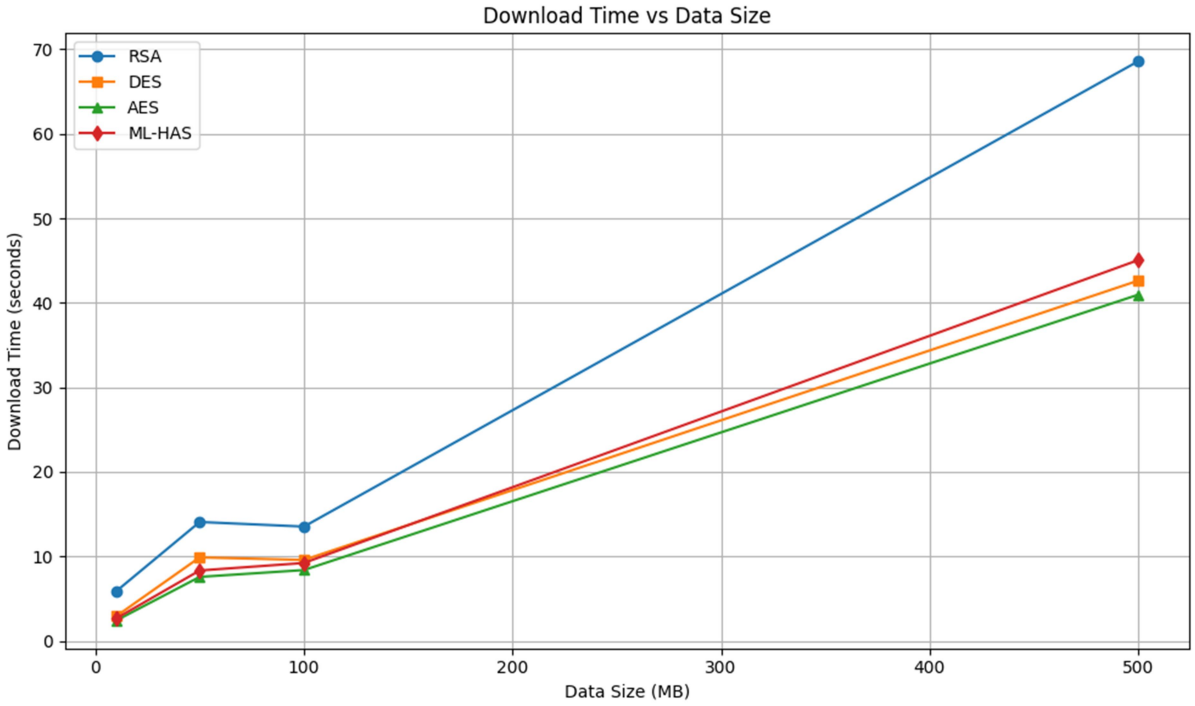


*Figure 9: Download Time Comparison*

In the above figure 9, RSA showed the slowest performance, taking nearly 69 seconds to download 500MB of encrypted data, which severely impacts overall system efficiency. DES and AES demonstrated significant improvements, with AES leading in speed among traditional algorithms. ML-HAS displayed a balanced and effective approach, achieving download times similar to AES and notably better than DES. For example, at 500MB, ML-HAS completed the download in about 45.05 seconds, compared to DES's 42.62 and AES's 40.96—showing competitive results. Notably, ML-HAS maintained a consistent rate of increase in download time, indicating scalability and reliability for growing data loads. These results affirm ML-HAS as a dependable and performance-efficient approach for encrypted data retrieval, ensuring that high-volume downloads can be executed quickly without bottlenecks. For modern applications requiring frequent and large-scale data access, such as cloud storage or video streaming, ML-HAS offers a practical and secure solution.

| **Security Property** | **How It Is Achieved** | **Explanation** |
|---|---|---|
| Confidentiality | Dynamic S-box and dynamic key generation to enhance AES encryption | Protects data from unauthorized access by encrypting it with symmetric keys that change per session, reducing susceptibility to brute-force and algebraic attacks. |
| Integrity | SHA-based hashing applied to each data slice | Ensures that each slice of encrypted data can be validated before reconstruction. Any tampering is detected using hash verification during decoding. |
| Availability | Information Dispersal Algorithm (IDA) for slicing data and enabling | Data is split into n slices with a recovery threshold m. Even if n - m slices are lost or corrupted, the original data can still be |

| | | |
|---|---|---|
| | threshold-based recovery | reconstructed. |
| Post-Quantum Resilience | Layered security approach combining AES, IDA, and hashing, avoiding reliance on vulnerable single-primitives | Unlike RSA and traditional AES alone, the framework resists future quantum attacks through its composite structure and data fragmentation. |
| Robustness to Data Loss | Redundant slicing with IDA and storage of multiple pieces across the cloud | Data remains recoverable even if some slices are inaccessible due to node failures or communication issues. |
| Secure Retrieval | Reverse transformation pipeline with integrity checks, slice reassembly, and decryption | During retrieval, data integrity is verified before slices are reassembled using IDA and decrypted, ensuring complete and authentic data restoration. |
| Multi-Dimensional Security | Combined use of encryption, fragmentation, and hashing | Achieves simultaneous protection of data from unauthorized access, unauthorized changes, and partial data loss — fulfilling the CIA triad effectively. |

*Table 5: Security Properties Achieved In The Proposed Framework*

Table 5 summarizes an overall view of the main security properties satisfied by the proposed Cloud Data Security Framework (CDSF) via its underlying (ML-HAS). The architecture is carefully crafted to meet the cloud security triad—confidentiality, integrity, and availability—as well as resilience to post-quantum threats and robustness to data loss. This contributes to making the proposed scheme resistant to classical and quantum cryptanalysis, ensuring confidentiality through improved AES encryption that utilises dynamic S-box and key generation mechanisms. SHA based hashing of each fragmented data slice ensures integrity by validating it before reconstruction. The Information Dispersal Algorithm (IDA) supports availability, dispersing the encrypted data into slices so that it can be recovered even if some of them are missing/corrupted. Furthermore, the layered transformation approach provides quantum-era survivability, as it avoids relying on any one cryptographic primitive. Secure retrieval occurs via a reverse decoding pipeline that ensures hash integrity, re-assembles the slices using IDA, and decrypts using AES. In summary, the proposed framework achieves the multi-dimensional security by combining encryption, data fragments, and hashing and thus providing an integrated and efficient approach, which can be an effective tool in the secure data outsourcing for modern and future cloud environments.

## 6. DISCUSSION

As cloud computing increasingly facilitates large-scale data storage and management, the need for data security against emerging post-quantum computational threats continues to rise. But now, conventional cryptographic schemes like AES, DES, RSA, etc, they do work against classical attacks, yet they are falling short because they can be broken using quantum algorithms. Existing solutions for resolving this challenge range from developing stronger encryption algorithms to hybrid solutions, but are still mainly incomplete against post-quantum threats, and they do not balance well either failover mechanism to maintain system resilience or from the perspective of unified security mechanism for confidentiality, integrity and availability (CIA).

This research highlights significant weaknesses in existing state-of-the-art cryptographic systems, which particularly rely on integrity-based approaches that lack versatility to quantum-era attacks and fail to provide secure data recovery and verification capabilities. As a method, we proposed a new hybrid scheme inspired by deep learning named the Cloud Data Security Framework (CDSF). In this method, enhanced AES based encryption, based fragmentation of SHA based hashing are implemented one after another forming a pipeline that offers better encryption, integrity verification and fault tolerant availability.

The performance of ML-HAS is validated through an empirical analysis by leveraging Amazon EC2 resources, which shows that ML-HAS strikes a good balance between increased security and lowered computational overhead. The additional overhead is negligible compared with AES, DES and RSA, while greatly enhancing post–quantum security features. The multilayered transformations in ML-HAS help to prevent single-point vulnerabilities while providing additional functionalities to resist potential adversarial attacks.

With using various security mechanisms, the proposed method solves some issues of previous techniques, such as dependence on a hard-coded single algorithm, no data verification and vulnerability to lost partial data. For practical use, this study can be extend to secure cloud storage solutions, specifically in fields that require significant data protection (e.g., healthcare, finance and government sectors). The results also confirm the robustness of the framework, and Section 5.1 presents the study limitations and recommendations for future improvements.

### 5.1 Limitations of the Study

While it is effective, the present study has some limitations. Second, the computational overhead due to multiple transformations can affect performance in realtime or resource-constrained environments in ML-HAS. Second, the framework has mostly been tested on structured data via Amazon EC2, which may limit its generalizability for other instances of unstructured or high-frequency data streams. Overall future works will improve efficiency of the execution, generalize to various dataset, add intelligent threat aware modules that improve adaptive security.

## 7. CONCLUSION AND FUTURE SCOPE

We proposed a new Framework of Cloud Data Security (CDSF) integrating Multi-Layer Hybrid Security Algorithm (ML-HAS) in this paper for the requirement of the pre-eminent security issue of data outsourcing in post-quantum era. Incorporating AES encryption, Information Dispersal Algorithm (IDA), and SHA hashing, the framework provides high confidentiality, integrity, and availability of data. Using Amazon EC2 for experimental, Results show the proposed approach offers more security than present cryptographic schemes (AES, DES and RSA) but it is still computationally inexpensive. By combining cryptographic transformations from multiple candidates, ML-HAS avoids single-bit vulnerabilities, allowing it to effectively resist more sophisticated attacks from classical computer and post-quantum threats. The rule applies most relevantly for cloud services used in sensitive sectors like healthcare, finance, and critical infrastructure. Nonetheless, this study itself has some limitations, and does not include real-time performance testing, is limited to structured data or services, and does not offer any implementations for adaptable learning components. Future work will focus on optimising the algorithm for real cloud environments, broadening the framework to cater for multiple data types, and integrating intelligent anomaly detection driven by deep learning to improve proactive threat response. With these enhancements, CDSF will be more scalable and adaptable for future cloud security ecosystems.

## REFERENCES

[1] FlevinaJoneseD'souza and DakshataPanchal . (2017). Advanced Encryption Standard (AES) Security Enhancement using Hybrid Approach. *IEEE*, p1-6.

[2] NishthaMathur , Rajesh Bansode . (2016). AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection. *Elsevier*, p1-8.

[3] Cheng-Hsiung Yang and Yu-Sheng Chien. (2020). FPGA Implementation and Design of a Hybrid Chaos-AES Color Image Encryption Algorithm. *MDPI*, p1-16.

[4] Marwan Adnan Darwish, EiadYafi, Mohammed A. Al Ghamdi and Abdullah Almasri. (2020). Decentralizing Privacy Implementation at Cloud Storage Using Blockchain-Based Hybrid Algorithm. *Springer*,p1-10.

[5] DivyaPrathana Timothy and Ajit Kumar Santra. (2017). A Hybrid Cryptography Algorithm for Cloud Computing Security . *IEEE*, p1-5.

[6] Salma,RashidahFunkeOlanrewaju, Khaizuran Abdullah, Rusmala and HerdiantiDarwis . (2018). Enhancing Cloud Data Security using Hybrid of Advanced Encryption Standard and Blowfish Encryption Algorithms. *IEEE*,p1-6.

[7] Vikrant Shende and MeghanaKulkarni . (2017). FPGA based Hardware Implementation of Hybrid Cryptographic Algorithm for Encryption and Decryption. *IEEE*, p1-4.

[8] Ye Liu, Wei Gong, Wenqing Fan. (2018). Application of AES and RSA Hybrid Alogrithm in E-mail. *IEEE*, p1-3.

[9] KhengKok Mar, ZhengQing Hu, Chee Yong Law, MeifenWa. (2016). Securing Cloud Data using Information Dispersal. *IEEE*, p1-4.

[10] BhushanAtote, Saniya Zahoor, MangeshBedekar and SujaPanicker. (2018). Proposed Use of Information Dispersal Algorithm in User Profiling. *Springer*, p1-11.

[11] Hassan Noura , Ola Salman , Ali Chehab , and Raphael Couturier. (2019). Preserving Data Security in Distributed Fog Computing. *HAL*, p1-26.

[12] Quan Qian, Zhi-ting Yu, Rui Zhang, Che-Lun Hung. (2018). A multi-layer information dispersal based encryption algorithm and its application for access control. *Elsevier*, p1-12.

[13] Marco Baldi, Alessandro Cucchiarelli, Linda Senigagliesi, Luca Spalazzi, Francesco Spegni. (2016). Parametric and Probabilistic Model Checking of Confidentiality in Data Dispersal Algorithms. *IEEE*, p1-8.

[14] KatarzynaKapusta, Gerard Memmi. (2015). Data protection by means of fragmentation in distributed storage systems. *IEEE*,p1-9.

[15] Vidyalakshmi B. S., Raymond K. Wong and Chi-Hung Chi. (2015). Privacy preserving information dispersal in social networks based on disposition to privacy. *IEEE*, p1-6.

[16] Amir M. Ahmadian , Maryam Amirmazlaghani. (2019). A novel secret image sharing with steganography scheme utilizing Optimal Asymmetric Encryption Padding and Information Dispersal Algorithms. *Elsevier*, p1-11.

[17] R. Guesmi · M. A. B. Farah, A. Kachouri and M. Samet. (2015). A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2. *Springer*, p1-15.

[18] FatmaKahri ,HassenMestiri, BelgacemBouallegue and Mohsen Machhout. (2017). AN EFFICIENT FAULT DETECTION SCHEME FOR THE SECURE HASH ALGORITHM SHA-512 . *IEEE*, p1-5.

[19] RavillaDilli and Dr Putta Chandra Sekhar Reddy. (2016). Implementation of Security features in MANETs using SHA-3 Standard Algorithm . *IEEE*, p1-4.

[20] Sandhya Verma and G.S.Prajapati . (2016). Robustness and Security Enhancement of SHA with Modified Message Digest and Larger Bit Difference . *IEEE*, p1-5.

[21] Moshira A. Ebrahim, Islam El Madahh, Hoda K. Mohamed . (2017). Hybrid Model For Cloud Data Security Using Steganography. *Researchgate*, p1-7.

[22] DilliRavilla and Dr Chandra Shekar Reddy Putta. (2015). Routing Using Trust Based System with SHA-2 Authentication . *Elsevier*, p1-8.

[23] Abhilash Ashok Bhadke, SurenderKannaiyan and VipinKamble. (2018). Symmetric Chaos-Based Image Encryption Technique on Image Bit-Planes using SHA-256. *IEEE*, p1-6.

[24] DASARI SHIVA KUMAR , L. SRINIVAS , P. V. N. SWAMY. (2015). Designing and Implementation of Secure Hash Algorithm-1(SH-1) . *IJVDCS*, p1-5.

[25] Kazys KAZLAUSKAS, Jaunius KAZLAUSKAS. (2009). Key-Dependent S-Box Generation in AES Block Cipher System. Institute of Mathematics and Informatics. 20(1), p.23–34.

[26] Fathy, A., Tarrad, I. F., Hamed, H. F. A., & Awad, A. I. (2012). Advanced Encryption Standard Algorithm: Issues and Implementation Aspects. Advanced Machine Learning Technologies and Applications, p516–523.

[27] Km. Amrita1 ,Neha Gupta2 ,Rashmi Mishra. (2018). AN OVERVIEW OF CRYPTANALYSIS ON AES. International journal of advance research in science and engineering. 7(1), pp.1-8.

[28] Garay, Juan A.; Miyaji, Atsuko; Otsuka, Akira (2009). [Lecture Notes in Computer Science] Cryptology and Network Security Volume 5888 || Linear (Hull) and Algebraic Cryptanalysis of the Block Cipher PRESENT. , 10.1007/978-3-642-10433-6(Chapter 5), p58–75.

[29] Gabriel A.J1 ., Alese B.K and Adetunmbi A.O3 ., Adewale O.S. (2014). Post-Quantum Crystography based Security Framework for Cloud Computing. Journal of Internet Technology and Secured Transactions (JITST). 3(4), pp.1-8.