A Hybrid Double Encryption Approach for Enhanced Cloud Data Security in Post-Quantum Cryptography

Manjushree C V[1], Nandakumar A N[2]
Information Science and Engineering, Vemana Institute of Technology (VTU University), Bangalore, India[1]
Computer Science and Engineering, VTU/City Engineering College, Bangalore, India[2]

***Abstract*—Quantum computers and research on quantum computers are increasing due to the efficiency and speed required for critical applications. This scenario also kindles the vitality of data protection needed against threats from quantum computers. Research in post-quantum threats is very minimal so far, but it is much needed to protect the enormous data stored in the cloud for healthcare, governmental, or any crucial data. This research work presents an advanced hybrid double encryption approach for cloud data security based on Post-Quantum Cryptography (PQC) to ensure the restriction of unauthorized access. The suggested approach combines the benefits of the NTRU encryption and AES encryption algorithms and works in hybrid mode, offering strong security while resolving issues with real-time performance and cost-efficiency. A streamlined key management system is set together to improve real-time processing, significantly reducing encryption and decryption delay times. Moreover, NTRU Encrypt dynamic parameter selection, which adapts security parameters based on data sensitivity, maintains accurate information and security. In addition to addressing real-time performance and data security, an innovative development in this method is known as Quantum-Adaptive Stream Flow Encryption (QASFE), which enables secure data sharing and collaborative working within a quantum-resistant framework. This innovative feature enhances data accessibility while maintaining the highest level of security. In the era of post-quantum cryptography, our multifactor authentication technique, integrating double encryption and QASFE, is a proactive and flexible solution for securing cloud data, and protecting data security and privacy against emerging threats.**

Keywords*—Cloud data security; double encryption; Post-Quantum Cryptography (PQC); NTRU Encrypt; AES Encryption

I. Introduction

Data security in the cloud has become essential in the present digital landscape as organizations depend upon increasing amounts on cloud-based services to safeguard, analyze, and manage their data. The cloud certainly radiates in three areas: scalability, accessibility, and cost-effectiveness. Data breaches, insider threats, and the ever-changing character of attacks are just a few of the specific security challenges that it additionally raises. Cloud computing technology has rendered it possible for many firms to design and deploy software with greater efficacy and effectiveness in the cloud, enabling savings on the expenses of purchasing and maintaining the infrastructure [1]. The term "cloud computing" refers to the idea of rapid, on-demand network access to a pool of programmable computing resources (including networks, storage devices, servers, apps, and services). It enables these assets to be delivered and released rapidly, with the least amount of managerial work and service provider engagement. Since security is the primary concern in cloud computing, some users may find themselves comfortable transmitting information via the cloud. Cloud computing specialists have created certain secret keys for account security and use encryption methods to safeguard cloud servers [2, 3, 5]. To safeguard the data from threatening attacks, specific encryption techniques might be employed. The cloud security posture is strengthened through frequent security assessments, incident response plans, and adherence to industry-specific laws and standards.

This research study was established by combining different security strategies to achieve the objective of cloud data security. Combining these techniques creates an obstacle against security issues, which have been preventing the cloud's acceptance and effective functioning. The field of cryptography has evolved in reaction to this impending quantum threat, which has contributed to the conception of Post-Quantum Cryptography (PQC). The major goal of PQC is to provide encryption techniques and cryptographic primitives that are resistant to quantum attacks. Attacks are computationally expensive and consequently ineffective as an outcome. These basic hypotheses, on which conventional stocks depend, are no longer valid with the development of post-quantum computing [4]. A shield against security issues that have frequently prevented the cloud from functioning and growing effectively is created by combining these techniques. Data security in the cloud utilizes a sophisticated strategy that combines innovative technology, widely accepted practices, and stringent regulations to safeguard data from unauthorized access, data breaches [5], and other cyber consequences of these challenges. One such cryptographic method combines NTRU Encrypt and AES encryption, resulting in an effective Double Encryption method. NTRU Encrypt, a lattice-based encryption system developed to withstand the cryptographic flaws that quantum computers can eventually exploit, is one of the notable PQC algorithms in this field. NTRU Encrypt, an effective encryption algorithm constructed on the mathematical underpinnings of lattice-based cryptography, is at the core of PQC's promise [6].

The Advanced Encryption Standard (AES) [7, 8] has evolved as an essential component of contemporary cryptographic methods in the pursuit of secure data transmission and storage. AES has become a cornerstone of data security in several industries owing to its dependability and effectiveness in protecting sensitive data. As the secondary

encryption layer, AES is essential to post-quantum cryptography and the idea of enhanced double encryption. It increases the quantum resistance offered by NTRU Encrypt and provides an additional level of security while also improving the impact and effectiveness of data protection as an entire.

Fig. 1 shows the essential steps in NTRU Encrypt and AES-based double encryption. It offers a strong security framework that makes use of the advantages of both encryption techniques to safeguard data in a way that is quantum-resistant while preserving computing effectiveness.

The following are the main contributions of this work:

- Post-Quantum Security: The primary contribution consists of implementing the post-quantum cryptography method, particularly NTRU Encrypt, to improve data security. It incorporates NTRU Encrypt, which is made resistant to quantum attacks, to address the immediate challenge that quantum computing presents to conventional cryptographic techniques.
- Double Encryption Strategy: Introduces a strong double encryption technique called the Double Encryption Strategy, which combines the advantages of the NTRU Encrypt and AES encryption techniques. Sensitive data is further protected with our dual-layered encryption strategy's extra degree of security.
- Key Management: Effective key management is essential for any encryption scheme, and the paper recognizes this by highlighting key generation as a significant contribution. It describes how to generate and manage cryptographic keys securely, which is crucial for the overall safety of the encryption system.

Quantum-adaptive Security: The primary benefit of this paper is the creation of quantum-adaptive security in the context of post-quantum cryptography. QASFE provides an unparalleled degree of adaptability and security by dynamically modifying encryption procedures based on the quantum threat level and data relevance.

This paper is structured as follows: Section II provides an overview of the literature review for the security of data in recent cloud computing research. Section III, a methodology is proposed to secure data prevention in cloud environments. Section IV presents the results and accompanying discussion, and Section V concludes this paper.

II. Literature Survey

A. Related Works

This section provides several recent cloud computing experiments. Even though many research efforts have focused on the security risks with cloud computing cryptographic techniques. Some researchers suggest employing innovative methods in addition to the strategies defined above to improve cloud computing security.

The literature review, which was conducted is provided in tabulated form (see Table I), provides an overview of the available work, and has established a ground for the proposed work. In this section, the approaches proposed by various researchers about the issue have been addressed for the recognition of the problem and understanding.

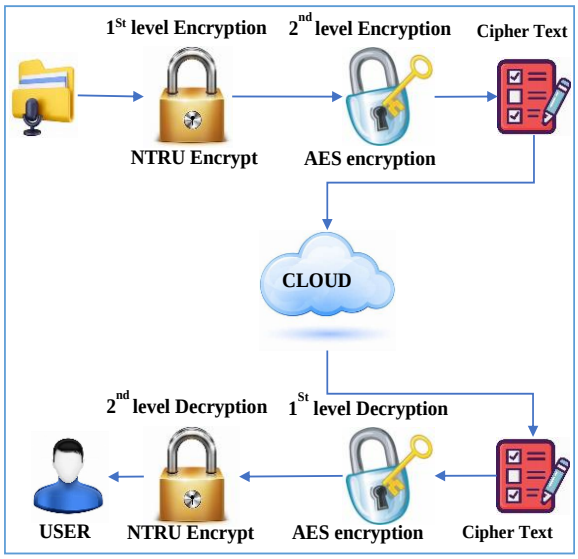

Fig. 1. Basic architecture for double encryption.

TABLE I. Analysis of Related Works

Reference	Focus	Description
Singh, Prabhdeep, and Ashish Kumar Pandey, et al. [9]	Data Security in Cloud	This study offers a thorough analysis of the literature on data encryption, data concealment, and data protection challenges, as well as solutions for cloud data storage. The effectiveness of each strategy is then contrasted based on its features, advantages, and drawbacks.
A. Malviya, R. K. Dwivedi, et al. [10]	Comparison of container orchestration tool	This research will assist professionals in determining if they require an orchestrator that is connected to a certain technology or one that offers an independent solution. Data integrity, availability, and secrecy are all referred to be forms of security, though. As long as they don't provide or guarantee this for this paperwork, there could be major issues.
Achar, Sandesh, et al.,[11]	Infrastructure as Code (IAC) across multiple clouds	This research indicates that there are a lot of challenges with managing the infrastructure provisioning of enterprise SaaS applications, including configuration drift and the variety of cloud providers. Without compromising on stability or quality, IAC makes it possible to roll out novel application architecture versions rapidly. Anytime a cloud host isn't accessible, there should be a warning period before the services restart.
Singh, A. K et al. [12]	Protecting the cloud data from unauthorized access	The researchers' proposed method complicates cryptanalysis by changing the plain text alphabet's position using prime numbers and then performing the hybrid RSA algorithm, which makes it more challenging to factorize the variable used in key creation. The main problem with employing is excessive resource utilization, which eventually results in higher costs and longer wait times.
Nejatollaji et al. [13]	Resistance against the dangers of quantum computing	This study examines trends in lattice-based cryptographic methods, including recent fundamental concepts for the use of lattices in computer security, difficulties in implementing them in software and hardware, and new

	in post-quantum cryptography.	requirements for their adoption. The survey also offered insightful ideas that would enable the reader to concentrate on the mechanics of the computation ultimately required for mapping schemes on already-existing equipment or generating a scheme in part or in full on specialized hardware.
Dutta, Aritra, et al., [14]	Multi-cloud storage's security for preventing unauthorized people from accessing data	According to this research, the business decides to utilize a username and password along with the NTRU encryption technique to encrypt the data to increase security. By doing this, it is possible to ensure that even if an attacker obtains access to the encrypted data, they will not be able to decrypt it without the correct password.
Harjito, Bambang, et al., [15]	Threats to the security of digital information	This study's findings demonstrate that the NTRU algorithm's key generation and encryption times are quicker than those of the RSA technique. The NTRU approach is better advised for cloud storage security because of its higher level of resiliency security. The NTRU algorithm, on the other hand, employs a lattice-based strategy with strong key selection and is also difficult to solve.
Costa, Bruno, et al. [16]	Security in the quantum universal composability	In this work, they propose randomized variants of two well-known oblivious transfer protocols, one quantum, and the other post-quantum, with ring training and an error assumption. The accuracy is sacrificed in preference to cost savings with these biometric authentication systems that have been reduced. This paper highlighted contemporary technological technologies like cloud computing, it is now possible to access data from any location.
Tarannum, Ayesha, et al. [17]	Data security method using multi-modal biometric sensing and authentication	To enable robust data integrity verification and data security in distributed applications, a new integrity computational algorithm and an encryption method have been developed in this work. As a result, each user receives a unique set of variable keys during the encryption process for additional security. This paradigm, however, is unable to provide the needed results in real time for multi-modal biometric authentication.

B. Motivation of the Proposed Research

As we've seen, a lot of research has been done on encryption, and in the majority of post-quantum cryptography research, the ranking operations are performed only on the platform side. Therefore, it is necessary to propose the PQC with NTRU-AES Encrypt.

III. Proposed Methodology

The adoption of strong post-quantum cryptographic solutions receives priority in the strategy due to the impending threat posed by quantum technology. The introduction of a revolutionary Double Encryption methodology, which combines the benefits of the NTRU Encrypt and AES encryption methods while including novel elements to improve data security and accessibility, is a key component of this strategy. Furthermore, it enhances key management processes to improve real-time performance, reducing encryption and decryption lag and enabling safe, on-the-fly data transfer and retrieval. This improved Double Encryption technique uses NTRU Encrypt and AES encryption for key generation to provide a diverse defense against potential quantum and classical attacks, which is necessary to combat the growing threat of quantum attacks. In addition, the methodology provides an innovative Quantum-Adaptive Stream Flow Encryption (QASFE) component that addresses temporal performance measurements and creates a simplified key management system to reduce latencies. This method offers a thorough and effective method for protecting data in the post-quantum era of cryptography while working to significantly reduce the time needed for encryption and decryption, ensuring security and real-time data accessibility. It does this by dynamically adjusting security parameters and adapting key sizes to data priority. An overview of a proposed methodology for improving data security in cloud systems is provided in Fig. 2. Strong Post-Quantum Cryptographic solutions are required as quantum computers approach. To address this issue, we provide a new Double Encryption technique that combines the benefits of NTRU Encrypt and AES encryption besides incorporating innovative components that improve data security and accessibility.

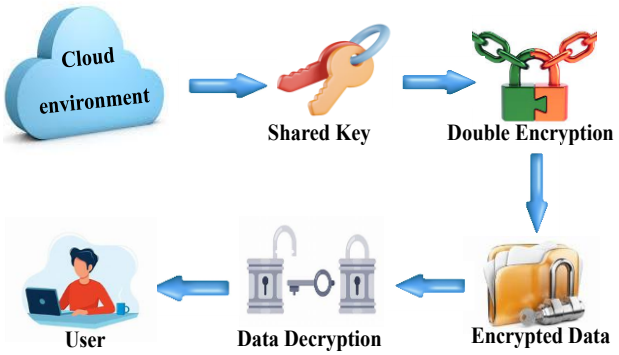

Fig. 2. Overview of proposed methodology for enhanced data security.

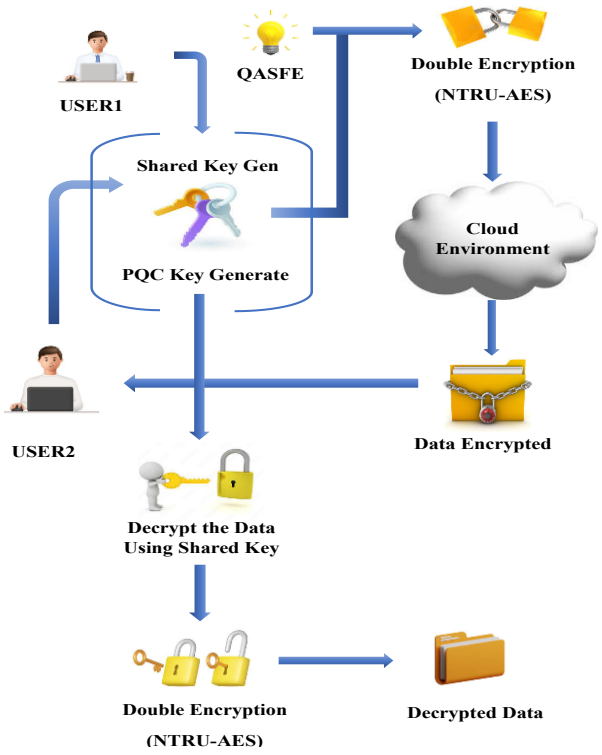

Fig. 3. Proposed architecture for double encryption data security.

To protect against quantum attacks, our enhanced Double Encryption method originates by using NTRU Encrypt and AES encryption for key generation. We optimize the key management procedure, though, to address queries regarding real-time performance. We want to decrease the latency of encryption and decryption by optimizing key generation and management. This would enable secure real-time data transfer and retrieval.

The combination of various cryptographic methods provides an effective defense against potential quantum attacks and classical attacks, improving the security posture generally. We aim to reduce the time needed for encryption and decryption by the optimization of the key generation procedure, enabling real-time data transfer and retrieval operations without sacrificing security. We add a unique component to our enhanced Double Encryption approach called Quantum-Adaptive Stream Flow Encryption (QASFE), which addresses the time performance measures. Due to the delay in period of time, our approach proposes a streamlined key management system that effectively creates and manages encryption keys to address this problem. Our approach, which relies on NTRU Encrypt and AES key generation, allows us to utilize smaller key sizes for high-priority data and larger key sizes for low-priority data to improve security. Our enhanced Double Encryption technique resolve the problems with real-time efficiency and also incorporates the revolutionary notion of Quantum-Adaptive Stream Flow Encryption (QASFE). We offer a comprehensive and effective method for protecting data in the era of post-quantum cryptography by enhancing key management, dynamically modifying security parameters, and implementing QASFE. Below Fig. 3, the proposed Double Encryption Data Security system is described. It combines NTRU Encrypt and AES encryption with a focus on quantum resistance, time efficiency, and data security in cloud environments. A strong and flexible security framework for the post-quantum generation is created by combining NTRU Encrypt, AES encryption, and the QASFE component.

A. NTRU Encrypt - AES Encryption

An asymmetric key (public - private key) and symmetric key (public key) cryptosystem termed the NTRU-AES encryption method is parameterized by three integers: (I, l, m), where p is greater than q, GCD (p, q) = 1, and N is prime. Polynomial rings P, Rp, and Rq should be considered. x^N-1 is an ideal in Z[x], that is, it contains all polynomials in H[x] that can be represented as multiples of a^I-1.

$$P = \frac{H[x]}{a^I-1}, R_p = \frac{\frac{Z}{P}H[x]}{a^I-1}, R_q = \frac{\frac{Z}{P}H[x]}{a^I-1}$$

The equation for the product of two polynomials a(x), b(x) ϵ R is given as

$$a(x) * b(x) = c(x)$$

$$C_K = \sum_{i=j=k\ (mod\ N)} a_i\ b_{k-i}$$

Here;

The variable on which the phrase C_K depends is K, which most likely denotes the result or output of this function.

The term inside the sum, $i = j = k\ (mod\ N)$, designates the range of values that the index variable i can take. For each value of i that meets the congruence criterion, the product of two sequences, $a_i\ b_{k-i}$, is contained within the summation.

To indicate any positive integers w1 and w2, let τ (w1, w2) denotes the set of ternary polynomials given by,

$$\tau\ (w1, w2) = \left\{ z(x) \in R \;\middle|\; \begin{array}{l} The\ d1\ coefficients\ of\ z(x)\ are\ equal\ to\ 1, \\ The\ d2\ coefficients\ of\ z(x) are\ equal\ to\ -1, \\ All\ other\ coefficients\ of\ z(x)\ are\ equal\ to\ 0 \end{array} \right\}$$

The polynomial z(x) with particular coefficient configuration composed the set τ (w1, w2). It includes polynomials with w1 coefficients of 1, w2 coefficients of -1, and w0 coefficients of 0. Based on these coefficient requirements, a set of polynomials can be defined utilizing this type of notation.

Key Generation: Implementing "NTRU-AES," a synergistic cryptographic technique that combines the mathematical efficacy of NTRU Encrypt for the generation of public and private keys with the dependability of AES for the generation of symmetric keys to produce a hybrid encryption system that provides unrivaled security in a quantum-resistant framework.

Choose private f(x) ϵ τ (w + 1, w)

Choose private v(x) ϵ τ (w, w).

- Generate f_Q (x) = f^{-1}(x) in R_q and f_p (x) = f^{-1}(x) in R_p
- Generate h (x) = f_q (x) * v(x) in R_q

Users' public keys are represented by polynomial h(x). Pair (f(x), f_p (x)) is the corresponding private key. The user can store only f(x) and regenerate f_p (x) from it. The encryption processes for plaintext m(x) ϵ R_p are indicated in the following phases.

Encryption: An essential part of encryption, and the security of the encryption protocol depends on the complexity of several mathematical challenges, such as the problem of encoding to obtain the cipher text message and the challenge of factoring the modulus employed in the polynomial ring.

- Select a random transitory key r(x) ϵ τ (w, w).

To perform this, employ an encoding technique that converts the message's plaintext to the ciphertext of the polynomial ring.

- Compute the ciphertext e(x) = pr (x) * h(x) + m(x) mod q.

The secure ciphertext matching the initial polynomial equation will be the result of adhering to NTRU and AES encryption (if used). The matching decryption method (which

undoes the stages of encryption) can be used to decrypt this ciphertext when required. It can be safely stored in the cloud.

Decryption: Data is transformed into an unreadable format using encryption algorithms and keys when it is encrypted before it is stored in the cloud. Authorized users or programs must decrypt the data to access and use it.

- Compute a(x) = f(x) * e(x) mod q
- Center lift a(x) to a(x) ϵ R
- Compute m = f_p (x) * a (x) mod p

Notably, the polynomial multiplication in the final decryption phase is omitted by selecting f(x) = 1+pf_1 (x), where f1 R in the key generation step as f_p = 1 mod p.

The overall result, m, is the message that has been decrypted. It is calculated by multiplying the result of f_p (x) by the modified a(x), then applying modulo p.

The precise perception and relevance of these operations will depend on the exact meanings of f(x), e(x), f_p (x), q, and p as well as the context in which this decryption procedure is utilized. The specifics of this procedure may vary based on the particular mathematical problem or cryptographic technique being used, although it is frequently observed in certain mathematical procedures and systems.

B. QASFE Framework

The real-time performance and data security in the cloud are enhanced by using the sophisticated mathematical framework of Quantum-Adaptive Stream Flow Encryption (QASFE). Lattice-based cryptography, a field of mathematics that involves solving difficult problems involving lattices, like the Shortest Vector Problem (SVP) and Learning with Errors (LWE), is the foundational idea of QASFE. To improve data security and manage real-time performance issues in cloud-based scenarios, lattice problems are exploited for their inherent computational complexity.

Lattice Basis: A group of vectors that are linearly separate that span a lattice, b1, b2, ..., bn, define the lattice as L:

$$\text{Lattice } L = \text{Span } (b1, b2, ..., bn)$$

$$L = \{x \mid x = \sum(ai * bi) \text{ for } ai \epsilon Z, 1 \leq i \leq n\}$$

In order to enhance the real-time performance of lattice-based cryptography, the aforementioned formula emphasizes improving the efficiency of lattice-based encryption and decryption, which is crucial for real-time performance:

$$O\ (D^3 * N * log^2\ (BS)) \quad (1)$$

Here:

L represents the lattice

x represents any vector that belongs to the lattice L, the symbol $\sum$ denotes summation,

ai represents integer coefficients.

bi represents basis vectors of the lattice.

Z represents the set of integers.

D represents the dimension of the lattice,

N is the number of lattice vectors.

BS is a bound on the size of the coefficients.

To optimize these parameters in Eq. (1) to enhance the real-time performance of lattice-based cryptography, it might be required to decrease the dimension, restrict the number of lattice vectors, or adopt lower parameter bounds. With the aid of these optimizations, encryption and decryption processes will be quicker and more effective.

Shortest Vector Problem (SVP): In a given lattice L, the Shortest Vector Problem (SVP) attempts to identify the shortest non-zero matrix as follows:

$$SVP(L) = \min \{||v|| \mid v \epsilon L, v \neq 0\}$$

$$TP = (2^d) / (SVP\ (L)^c) * \log2(N) \quad (2)$$

where,

SVP(L) represents the lattice's average shortest vector length L.

min {||v|| | v ϵ L, v ≠ 0} signifies the search for the minimum Euclidean norm (length) of a non-zero vector v within the lattice L, 2^d represents the dimensionality of the lattice's parabolic expansion in computational complexity.

log2(N) represents the performance impact of basis size is expressed by the logarithm of the number of lattice basis vectors with base 2,

Eq. (2) describes the dimension of the lattice, the average shortest vector length, the number of basis vectors, and the computing difficulty of solving the SVP in a lattice-based cryptographic system.

Learning with Errors (LWE): LWE utilizes an error e from a particular distribution D in conjunction with a vector s from Z q^n.

Finally, a set of noisy linear equations is computed:

a = (a1, a2, ..., an) ∈ Z q^n

b = <a, s> + e mod q

a ← Uniform polynomial in R q.

e ← Error polynomial in R q.

b = a*s + e

ciphertext = (a, b)

where,

'a' is a vector containing 'n' integers from the ring Z q.

's' is a secret vector (usually known only to the recipient of the ciphertext).

'e' is a noise term introduced to enhance security.

'<a, s> ' represents the dot product of 'a' and 's'.

The result 'b' is computed as the dot product plus the noise term, all taken modulo q.

ciphertext = (a, b) represents the result of the LWE encryption process.

This encryption procedure adds some noise ('e') to the ciphertext in the context of LWE, rendering it extremely difficult for attackers to extract the private vector's' from the ciphertext. Even with the use of innovative quantum techniques, it is difficult for attackers to separate the original plaintext from the ciphertext due to the inclusion of erroneous phrases in the encryption process.

From QASFE, the mathematical foundations of lattices, which include the Shortest Vector Problem (SVP) and Learning with Errors (LWE), enhance their resistance to quantum attacks. A scenario where data remains private and secure in the cloud has become possible due to the adoption of such secure cryptographic techniques, which become increasing essential as quantum computing develops.

IV. Results and Discussion

The proposed Double Encryption methodology has undergone thorough evaluation and testing. It combines NTRU Encrypt and AES encryption and is enhanced by the innovative QASFE component. In this instance, we examined the data security strategy, focusing on crucial performance indicators like entropy and throughput. The implementation was performed using Python programing language.

The table illustrates various settings for entropy, and throughput. The comparison of several algorithms is shown in Table II along with relevant metrics including the proposed method's entropy and encryption and decryption time.

TABLE II. Comparing several Techniques based on Variables Like Entropy, Encryption Time, and Decryption Time

Methods	Average entropy per byte	Throughput (kb/sec)
AES	3.840	192.00
RSA	3.095	100.06
BLOWFISH	3.892	197.20
PROPOSED	7.440	237.12

A. Entropy

The term "entropy" refers to a gauge of the random or unpredictability of data in the setting of data security and cryptography. Higher entropy values imply that the method of encryption is more advanced and secure since it becomes more difficult for a competitor to predict or decode the encrypted data. The average entropy per byte for several encryption techniques is shown in Fig. 4, providing insight into the level of data protection for every strategy. Particularly, the proposed method far outperforms the competition, sporting high average entropy per byte of 7.44, indicating a significant improvement in data security compared to the conventional encryption techniques.

B. Throughput

It is a metric for gauging the way effectively processors respond to an algorithm. The volume of data transferred between users serves as a measure of it. The file uploading phase must have a high throughput that allows for the transfer of all data. When uploading files, the proposed approach displays the highest throughput.

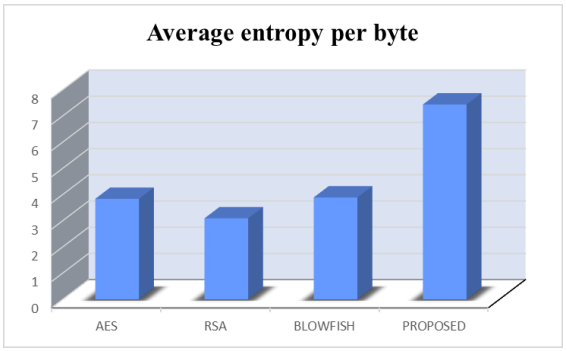

Fig. 4. Average entropy values of proposed model with existing AES, RSA and Blowfish algorithm. (x-axis: unit per byte, y-axis: Various encryption techniques).

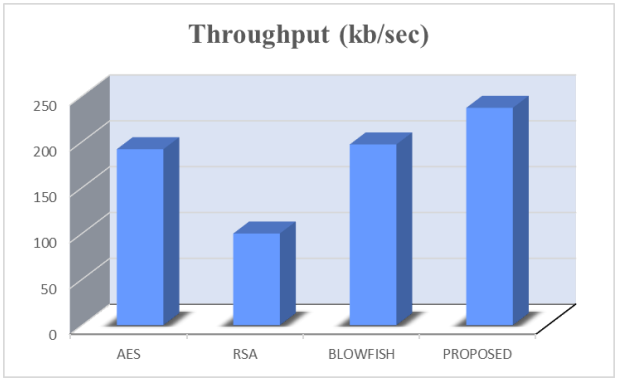

Fig. 5. Throughput values of the proposed model compared with existing AES, RSA, and Blowfish algorithm (x-axis: kB/s, y-axis: Various encryption techniques).

Fig. 5 compares the throughput of various cryptographic techniques, such as AES, RSA, and BLOWFISH, in kilobytes per second (kb/sec), with the proposed method. The proposed technique shines apart by possessing a higher throughput of 237.12 kb/sec, indicating the speed with which it processes data. These results imply that the proposed strategy demonstrates superior data processing abilities, making it an appropriate pick for applications that require both security and performance.

V. Conclusion

In conclusion, our suggested data security design offers a significant progress in the field of cloud security and data protection, specifically in considering recent developments in quantum computing. We have improved data security along with addressing critical concerns regarding real-time performance and computational prosperity by developing an innovative Double Encryption technique that combines NTRU Encrypt with AES encryption and the quantum-resistant properties of Post-Quantum Cryptography (PQC), offering an effective defense against the evolving threats and challenges of the digital era. Our core innovations, such as the unique QASFE, dynamic security parameter modifications, and improved key management, accessible the path for a data security system that is more time-sensitive, resource-effective, and resilient. This study reimagines the data protection

environment by giving enterprises a strong, flexible, and quantum-resistant solution that enables them to protect their most important data while ensuring quick and secure data transfers.

REFERENCES

[1] Jones, Kofi Immanuel, and R. Suchithra. "Information Security: A Coordinated Strategy to Guarantee Data Security in Cloud Computing." International Journal of Data Informatics and Intelligent Computing 2.1 (2023): 11-31, 2023.

[2] Kulshrestha, Vartika, Seema Verma, and C. Rama Krishna. "Hybrid probabilistic triple encryption approach for data security in cloud computing." International Journal of Advanced Intelligence Paradigms 21.1-2, 158-173.

[3] Gupta, Ishu, et al. "Compendium of data security in cloud storage by applying hybridization of encryption algorithm", Institute of Electrical and Electronics. Engineers (IEEE), 2022.

[4] Alu, Esther S., Kefas Yunana, and Muhammed U. Ogah. "Secured Cloud Data Storage Encryption Using Post-Quantum Cryptography." International Journal of Advanced Research in Computer and Communication Engineering. Vol. 11, Issue 7, July 2022.

[5] Devi, B. Padmini, and S. Kannadhasan. "Preventing Data Leakage in Cloud Servers through Watermarking and Encryption Techniques." Research Square, 2023.

[6] Ukwuoma, Henry C., et al. "Quantum attack-resistant security system for cloud computing using lattice cryptography." International Journal for Information Security Research 12.1, 2022.

[7] Alemami, Yahia, et al. "Cloud data security and various cryptographic algorithms." International Journal of Electrical and Computer Engineering 13.2, 2023.

[8] Fatima, Sana, et al. "Comparative Analysis of Aes and Rsa Algorithms for Data Security in Cloud Computing." Engineering Proceedings 20.1, 2022.

[9] Singh, Prabhdeep, and Ashish Kumar Pandey. "A Review on Cloud Data Security Challenges and Existing Countermeasures in Cloud Computing." International Journal of Data Informatics and Intelligent Computing 1.2, 23-33, 2022.

[10] A. Malviya and R. K. Dwivedi, "A Comparative Analysis of Container Orchestration Tools in Cloud Computing," 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, pp. 698-703, 2022.

[11] Achar, Sandesh. "Enterprise SaaS Workloads on New-Generation Infrastructure-as-Code (IaC) on Multi-Cloud Platforms." Global Disclosure of Economics and Business 10.2, 55-74, 2021.

[12] Gupta, I., Gurnani, D., Gupta, N., Singla, C., Thakral, P., & Singh, A. K., "Compendium of data security in cloud storage by applying hybridization of encryption algorithm", Institute of Electrical and Electronics Engineers (IEEE), 2022.

[13] Nejatollahi, Hamid, et al. "Post quantum lattice-based cryptography implementations: A survey." ACM Computing Surveys (CSUR), 51.6, 1-41, 2019.

[14] Dutta, Aritra, et al. "A New Encryption Algorithm Helps to Secure the Cloud Storage." International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 16, Number 1, 2023.

[15] Harjito, Bambang, et al. "Comparative Analysis of RSA and NTRU Algorithms and Implementation in the Cloud." International Journal of Advanced Computer Science and Applications 13.3, 2022.

[16] Costa, Bruno, et al. "Randomized Oblivious Transfer for Secure Multiparty Computation in the Quantum Setting." Entropy 23.8, 1001, 2021.

[17] Tarannum, Ayesha, et al. "An efficient multi-modal biometric sensing and authentication framework for distributed applications." IEEE Sensors Journal, 20.24, 15014-15025, 2020.