

Data security challenges and its solutions in cloud computing through quantum resistant advanced encryption standards

Govind Murari Upadhyay [†]

Department of Computer Applications

Manipal University Jaipur

Jaipur 303007

Rajasthan

India

Rashmi Priya

Department of Computer Science and Engineering

K R Mangalam University

Gurugram 122103

Haryana

India

Mukesh Joshi

Department of Computing

Graphic Era Hill University

Bhimtal Campus 263136

Uttarakhand

India

Meenakshi Narula

Department of Information Technology

Jagannath International Management School

New Delhi 110070

India

Prashant Vats

Department of Computer Science

Manipal University Jaipur

Jaipur 303007

Rajasthan

India

[†] E-mail: govind.upadhyay@jaipur.manipal.edu

Pramod Kumar Soni *

*Department of Computer Applications
Manipal University Jaipur
Jaipur 303007
Rajasthan
India*

Abstract

Assuring data security and communication integrity and limiting unauthorized access to critical data via public networks are now the most prevalent security concerns in cloud servers. We address these problems by introducing a secure data access and storage method that uses Quantum Resistant Advanced Encryption standards (QRAES) encryption algorithm on data blocks to safeguard both keys and data. To maintain data transmission security, it employs an alternative interpretation of Advanced Encryption Standards. Furthermore, certified safe key creation with low time complexity uses a shared secret that is provided by Diffie Hellman (DH). Furthermore, to protect against data loss and corruption due to insiders in the cloud, an Optimized Swarm Intelligence Algorithm (SIA) is used; this algorithm effectively recovers and restores any lost data. To maintain the confidentiality and integrity of sensitive data, the proposed system lays out and authenticates the path for safe data, addressing access security issues in cloud data storage and access.

Subject Classification: 68U35.

Keywords: Cloud computing, QRAES, Diffie hellman (DH), Swarm intelligence algorithm.

1. Introduction

With its unmatched scalability, flexibility, and affordability for a wide range of applications, cloud computing (CC) has emerged as a game-changing technology with enormous influence. Despite its widespread acceptance, many people remain concerned about security lapses and illegal access, particularly in cases where sensitive data has been transferred to distant shared servers. From a security perspective, CC is intrinsically dangerous due to its shared resource paradigm [1,2]. Encryption methods are necessary to protect data confidentiality during storage and transfer. Advancements in encryption algorithms like AES (Advanced Encryption Standards) [3], homogeneous encryption, and RSA (Rivest-Shamir Adleman) have been studied to protect sensitive data even in the event of security breaches. For controlling data access in cloud environments, access control solutions are just as important as encryption. Through the

* E-mail: Pramod.soni@jaipur.manipal.edu (Corresponding Author)

prevention of unauthorized users from accessing cloud systems, authentication, and identity management contribute to their integrity [4,5].

To understand the collaborative cloud services and the dynamic multi-tenant environment, visualization technologies are required to provide strong isolation tactics. These techniques are required to stop unauthorized access to virtual instances operating on the same physical server and safeguard sensitive data by averting cross-tenant breaches. New safety measures are being researched in response to edge computing's growth to adjust to the changing cloud environment and provide data security while accounting for factors like reduced latency, increased efficiency, and various forms of physical security close to the data source [6, 7]. To address significant data security challenges in cloud computing, this study developed the Quantum Resistant Advanced Encryption Standards (QRAES) for dependable data and key protection and Diffie Hellman for safe key production. By preventing data corruption, an enhanced Swarn Intelligence Algorithm (SIA) increased the resilience of cloud insider threats. The recommended approach effectively resolves security concerns related to cloud computing by guaranteeing secure data access, identity, and integrity.

2. Related Work

A technique for hybrid cryptography was introduced to improve CC data security [8] that integrates symmetric and asymmetric encryption techniques to provide dependable and efficient data protection in cloud environments. Challenges posed by the specific cloud environment, concentrating on issues with vulnerability management, data protection, and identification are investigated [9]. The study proposed a novel approach to enhance cloud-based storage security by employing a hybrid encryption technique and provides the advantages of symmetric and asymmetric encryption techniques and enhanced data security. The study [10-11] looks at the challenges and importance of security and privacy concerns in cloud computing. It talks about the challenges cloud systems have with user privacy and data security. The article covers several security and privacy-related topics while looking into the larger issues that need to be tackled in this changing environment. The study investigated security concerns related to cloud computing. When offering risk reductions, it covered a wide range of challenges and probable flaws in cloud computing settings. They emphasize the importance of safeguarding data, privacy,

and access control in cloud systems to better comprehend cloud computing security.

The study looked at issues with data security and privacy in fog computing applications. The study investigates ways to protect sensitive data and is centered around fog and cloud computing platforms made for Internet of Things (IoT) applications. They examined key tactics and challenges related to guaranteeing data safety in this distributed and decentralized computing paradigm. The study included cloud data security and looked at several cryptographic techniques. The focus was on enhancing the safety of information stored on cloud servers. They looked at numerous encryption techniques to lower the risk to security and ensure the integrity and confidentiality of sensitive data. This paper provides information on cloud computing data security utilizing cryptographic approaches.

Data security and privacy issues in fog computing applications are investigated. The research examines techniques for safeguarding sensitive data and is centered around fog and cloud computing platforms intended for Internet of Things (IoT) applications. They looked at key tactics and challenges associated with guaranteeing data security in this distributed and decentralized computing paradigm. Along with discussing cloud data security, the study looked at several cryptographic techniques. The primary focus was enhancing the safety of information stored on cloud storage. They looked at several encryption techniques to lower any security risks and ensure the integrity and confidentiality of critical data. To safeguard data in cloud computing, the paper provides information on cryptographic approaches.

3. Methodology

3.1 *Quantum Resistant Advanced Encryption Standard (QRAES) Encryption Algorithm*

The Advanced Encryption Standard (AES) is a special architecture that may be used in both software and hardware contexts to encrypt and decrypt sensitive data. In essence, it offers a particular framework for secret data encryption and decryption. This technique uses a 128-bit data block with a key length that is not 128, 192, or 256-bit in length. The algorithm's name changes based on the size of the key; it can have the notation QRAES-128, QRAES-192, or QRAES-256. Depending on the key diminution, different rounds or phases of the encryption and decryption

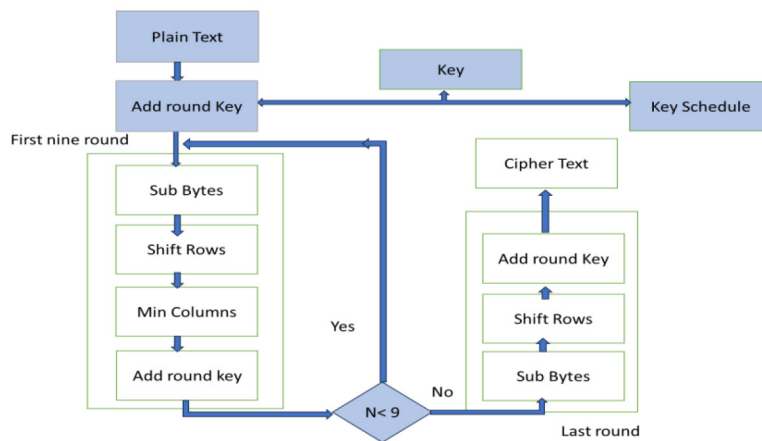


Figure 1

The procedure of Advanced Encryption Standard (AES)

process were used. QRAES uses four primary changes to encrypt data: replacing bytes, moving rows, mixing columns, and rounding keys. In brief, the encryption process involves the following steps:

1. Replacing bytes: An S-box lookup table was used as the foundation for a nonlinear byte substitution.
2. Moving rows: The number of cycles that the state's rows underwent was specified.
3. Mixing columns: The state's columns were mixed, with four bytes in each column, as part of the mixing step.
4. Adding a round key: A key schedule was used to combine state bytes with the round key that was generated from the cipher key.

Each of these components' inverses QRAES employed Inverse Substitution bytes, Inverted Shift Rows, and Inverted Mix Columns in its encryption process. Figure 1 illustrates how the complete process was carried out, including encryption and decryption.

3.2 Key Distribution Using Diffie Hellman (DH) with QRAES

The most important component of secure communication was key distribution, which was often accomplished by the Diffie Hellman (DH) key exchange in conjunction with QRAES.

3.2.1 Diffie Hellman (DH) Key Exchange

The Diffie Hellman (DH) method of key exchange allows two parties via an insecure communication channel to formulate a shared secret key without disclosing the secret to each other. With this shared information, a symmetric encryption key for confidential communication can be generated.

3.2.2 Encryption by using QRAES

The sender and receiver can use the shared secret as a symmetric encryption key, such as AES, once they have created it via DH. AES was a block cipher that worked on fixed-size data segments and was very secure when used with the correct key. The sender and receiver can choose a specific mode of operation for QARES, such as GCM or CBC, depending on their requirements. They can use the established shared secret as the encryption and decryption key for AES. Sender and receiver now can securely exchange encrypted messages using QRAES, knowing that the shared secret they delivered through DH was serving as the key.

3.3 Data Restoration through Utilization of SIA

Our method uses the Optimized Swarn Intelligence Algorithm (SIA) to restore data thoroughly and efficiently. SIA dynamically coordinates an effort among intelligent agents to restore lost data precisely and swiftly when it is lost or corrupted in cloud storage. By making use of Swarn's collective intelligence, SIA expedited the restoration process, guaranteeing minimal downtime and safeguarding against any data vulnerabilities, thereby enhancing the cloud storage system's resilience and dependability.

The social behavior of humpback whales served as the model for the Whale Optimization Algorithm (WOA), an optimization technique. It is like how whales hunt in groups, with the oldest whale guiding the group to the kill. This method has been adjusted to handle optimization concerns, like cloud computing data security concerns. The Whale Optimization Algorithm consisted of three main stages: search, bubble net feeding, and encirclement of the victim.

Initialization: Create a population of potential fixes (security configurations) that were displayed as whale positions.

Search: In this phase, the whales scour the search area in search of potential answers. Each whale stands for a potential answer. Position of the whale (solution candidate)

$$X_i = X_{i1}, X_{i2}, X_{i3}, \dots, X_{id} \quad (1)$$

Where d was the dimensionality of the problem.

Bubble-net Feeding: Whales create a bubble-net to catch prey during this stage. This behavior promotes convergence towards a viable solution.

$$X_{new} = X_{current} - A \times D \times (X_{best} - X_{current}) \quad (2)$$

Where the modified position of the whale is X_{new} . The whale's location currently at $X_{current}$ and A is the coefficient that gets smaller as iterations progress. D is the separation between the current whale and the leader whale, which offers the optimal solution

Pray Encirclement: Whales swim in circles around their prey during this stage. This aids in focusing the search and locating the ideal resolution.

$$X_{new} = X_{best} - A \times C \times (X_{rand} - X_{current}) \quad (3)$$

Where C was a chance number between $[0,1]$, the position of the selected random whale was X_{rand} .

Handling Boundaries: Make that the revised whale locations are combined inside the solution space's outlined boundaries.

Stopping Standards: When a predetermined number of iterations have been completed or a workable solution has been identified, the algorithm terminates.

The whale optimization algorithm seeks to minimize vulnerabilities and hazards by interactively performing these steps to optimize security setups for cloud computing data protection.

4. Result and Discussion

Aneka uses the Windows OS-compatible Python platform. Its unique emphasis on forward-thinking technological metrics is what makes it stand out from more widely accessible solutions. The user interface is the Aneka management studio, which provides computing and storage services customized to meet our research needs. The performance of the proposed framework is analyzed on the following parameters.

4.1 Encryption Time

An encryption algorithm's encryption time is the amount of time needed to transform plain text into ciphertext. In terms of data encryption using the anticipated framework and an effective SIA technique, the time

needed to encrypt the data was directly correlated with the encryption process.

$$\text{Encryption Time} = C_T / R_T \quad (4)$$

The term “Encryption Time” refers to the length of time required to finish encryption the terms “encryption computation time” (CT) and “encryption response time” (RT) denote this.

4.2 Decryption Time

A decryption algorithm transforms encrypted text (ciphertext) into readable text (plaintext) throughout a predetermined amount of time known as decryption time. The proposed framework explicitly links the decryption operations to the time required to decrypt the data.

$$\text{Decryption Time} = d_t / s_t \quad (5)$$

In this case s_t was the duration of processing a decryption request, and d_t was how long it takes to run the decryption calculation. Table 1 depicts the time required for the decryption and encryption process in the suggested framework and Table 2 Illustrates the methods, both proposed and existing, utilizing different parameters.

Table 1
Time required for the decryption and encryption process in the suggested framework.

Size of file (kb)	Time for encryption (ms)	Time for decryption (ms)
21	290	285
46	300	290
71	310	310
84	318	320

The effectiveness of the suggested and current methods was assessed the terms of encryption, decryption, time complexity, run time, and average latency. Multiparty Quantum Key Distribution (MQKD), Multi-level Authentication Technique (MLAT), and Quantum Key Distribution (QKD) were existing processes compared to the proposed method.

Table 2
Analysing the methods, both proposed and existing, utilizing different parameters.

Methods	Encryption (ms)	Decryption (ms)	Time complexity (ms)	Run time (ms)	Average latency (ms)
MQKD	356	350	506	480	700
MLAT	384	360	544	56	786
QKD	307	305	504	406	603
QRAES (Proposed)	305	302	501	403	600

5. Conclusion

The protection of communication integrity and limiting unauthorized access to private information transferred over public networks are the two main security concerns. Our innovative approach circumvents these challenges by employing the QRAES algorithm, which secures data blocks by encrypting the encryption key and the contents, guaranteeing safe storage and retrieval. Rethinking the Advanced Encryption Standards increased the security of data transit. We used the Optimized SIA to address insider threats that cause data loss or corruption since it efficiently recovers lost data and minimizes damage. By guaranteeing authentication and laying the foundation for safe data access via the application of comprehensive architecture, our solution effectively handles the range of security concerns associated with cloud data storage. This multi-layered security technique protects sensitive data from potential threats by combining access controls, authentication protocols, and encryption to ensure its purity and secrecy. Complicated encryption may have an impact on processing performance. Using AI with blockchain technology to detect threats dynamically and increase immutability.

References

- [1] Yenugula, M., S. Sahoo, and S. Goswami. "Cloud computing in supply chain management: Exploring the relationship." *Management Science Letters* 13.3 (2023).
- [2] Thabit, Fursan, et al. "Data security techniques in cloud computing based on machine learning algorithms and cryptographic algorithms:

Lightweight algorithms and genetics algorithms." *Concurrency and Computation: Practice and Experience* (2023).

- [3] Ukwuoma, Henry Chima, et al. "Post-quantum cryptography-driven security framework for cloud computing." *Open Computer Science* 12.1 (2022).
- [4] Roslin Dayana, K., and P. Shobha Rani. "Trust aware cryptographic role-based access control scheme for secure cloud data storage." *Automatika* 64.4 (2023).
- [5] Pan, Tian, et al. "Sailfish: Accelerating cloud-scale multi-tenant multi-service gateways with programmable switches." *Proceedings of the 2021 ACM SIGCOMM 2021 Conference*. (2021).
- [6] Khan, Mujahid. "Edge Computing: Extending the Cloud to the Edge of the Network." (2023).
- [7] Poonia, Ramesh C., and Linesh Raja. "On-demand routing protocols for vehicular cloud computing." In *Research Anthology on Architectures, Frameworks, and Integration Strategies for Distributed and Cloud Computing*, pp. 96-122. IGI Global, (2021).
- [8] Sun, PanJun. "Security and privacy protection in cloud computing: Discussions and challenges." *Journal of Network and Computer Applications* 160 (2020).
- [9] Saini, Satnam Singh, et al. "Automatic irrigation control system using Internet of Things (IoT)." *Journal of Discrete Mathematical Sciences and Cryptography* 25.4 (2022).
- [10] Malik, Medhavi, et al. "High level browser security in cloud computing services from cross site scripting attacks." *Journal of Discrete Mathematical Sciences and Cryptography* 25.4 (2022).
- [11] Upadhyay, Govind Murari, and Shashi Kant Gupta. "An Approach for Optimal Placement of Data in Fog Computing." *Turkish Online Journal of Qualitative Inquiry* 12.8 (2021).