International Journal of Emerging Multidisciplinary Research And Innovation (IJEMRI)

Quantum-Inspired Algorithms for Secure Cloud Data Migration and Encryption

[1]Ranganathan S, [2]Dr S. Radhakrishnan
[1]Research Scholar,
PG& Research Dept of Computer science,
Nehru Memorial College (Autonomous), Affiliated to Bharathidasan University,
Puthanampatti, Trichy Tamil Nadu.
[2]Associate professor & AI Researcher
Department of management , Debre Berhan University, Ethiopia.
sradhainboxs@gmail.com, Mobile : +251 983110070

ABSTRACT

The necessity to provide the effective and secure data migration processes is growing inexorably because of the fact that cloud computing is being created as the foundation of the modern digital ecosystems. However, the conventional encryption and migration algorithms are challenging in the ability to resist the quantum computing attacks that currently exist and offer security at real-time. In this paper, quantum based hybrid encryption system of safe cloud data transfer has been proposed. The framework embraces the quantum key distribution (QKD) concepts, optimization of chaotic map and generates keys with the help of the genetic algorithm to carry out the high speed and adaptive encryption. The simulated transfers of the data between the nodes of the cloud data have proved that the cloud data encryption solidity and the time lag is 47 and 31 less than the traditional AES and RSA systems respectively. One of the most probable pre-quantum defence technologies which will allow the data to be transferred safely and successfully in the case of the dynamic cloud infrastructures is quantum-inspired computing as it is revealed in the present paper.

Keywords: *Quantum-Inspired Computing, Cloud Security, Data Migration, Hybrid Encryption, Cryptography.*

DOI: https://doi.org/10.65180/ijemri.2025.1.3.02

Introduction

Cloud computing has been a revolution of applying storage and processing of information by provision of scalable and distributed networks. Nonetheless, the increasing amount of data and user dependence make the issue of security threat during the migration and storing an emergency (Zhou et al., 2022). The quantum attack will compromise even the current encryption algorithms of AES-256 and RSA algorithm due to the availability of other algorithms such as Shor and Grover algorithms that can break cryptographic keys exponentially (Rao and Chen, 2021).

Although quantum cryptography provides an unconditional security, this is provided to the condition that the hardware is quite costly and the infrastructure is not that developed. Therefore, quantum-inspired algorithms (QIAs) quantum-mechanism-inspired non-quantum algorithms that are guided by the mathematical principle of superposition, entanglement and probability amplitude provide a promising and feasible way of addressing quantum-level safety in a classical world (Liu et al., 2023). The researcher in the article develops a Quantum-Inspired Hybrid Encryption and Migration Framework (QIHEMF) of the secure, dynamically and efficiently transferring data in the multi-cloud architecture. It is a simulator, which emulates the dynamics of quantum states to produce key and heuristically optimization in the dynamic development of encryption key.

Background of the Study

The reason is that the pace of the increase in cloud-based enterprise applications, data analytics, and Internet of Things (IoT) services is large and must be ensured with inter-cloud transfer protocols of data. However, the heterogeneous platform data flow will most likely cause the data leakages, the man-in-the-middle attack, and the vulnerability of the algorithm (Patel et al., 2021). Explored how digitalization has revolutionized the banking sector through automation, online transactions, and the adoption of emerging technologies. The study highlighted that digital transformation improves operational efficiency, enhances customer experience, and promotes transparency in financial services. It also emphasized that the integration of digital tools has redefined traditional banking models, paving the way for innovation and technological advancement across industries Deshpande (2018).

Cryptography has some problems and opportunities presented by quantum computing. Despite the security threat that quantum algorithms pose to classical encryption, quantum algorithms can be applied to develop new principles on the safe computation (Wang et al., 2022). Quantum-inspired computing and attempts to replicate quantum-like behaviours i.e. stochastic superposition and probabilistic transitions in contrast to the conventional computational resources (Singh and Kumar, 2023). In order to mitigate the manifested security weaknesses, the paper proposes quantum-inspired Encryption Framework based on quantum-inspired key scheduling, entropic randomisation and multi-layer hash authentication.

Justification

It now has non-adaptable and quantum resistant decryption friendly encryption methods that are computationally intensive (Liu et al., 2023). The research community is extremely seeking scalable pre-quantum solutions, to allow them to secure their systems until such a time when the infrastructure is fully constructed to full quantum. The rationale employed to argue in favour of this research is pegged on the following three facts:

Technological relevancy Future problems of secure cloud system.

Operation performance: One has to reduce the duration of the migration and the encryption integrity should not be lost.

Ethical and regulation compliance: The alignment of the data privacy to such international standards as GDPR, ISO /IEC 27018, or the roadmap of post-quantum cryptography devised by NIST (NIST, 2023).

In that manner, the provided framework will represent the compromise between the classical and the post-quantum encryption requirements.

Objectives of the Study

The goal is to come up with a quantum-inspired hybrid encryption algorithm so as to accomplish the safety of cloud data migration.

To generate generation of key quantum-like of probabilities to enhance the cryptographic skills.

To compare the latency, throughput and strength with the traditional algorithms.

To provide a map of application of the quantum-inspired techniques in the future cloud systems.

Literature Review

Previously, the privacy of cloud migration is connected with the application of encryption and virtual private networks. According to Zhou et al. (2022), the insecure data transfer protocol is the one that insecurely generates over 65 percent of the cloud vulnerabilities.

Rao and Chen (2021) explained how the Shor algorithm may compromise the RSA by means of factorization of large primes and the Grover algorithm may compromise the power of the symmetric cryptography by cutting the key size by half.

Superposition simulation on optimization problems Wang et al. (2022) demonstrated that the optimization problem could be simulated using QIAs. The strength of the brute-force security of the study by Singh and Kumar (2023) against the dynamism of the key evolution used in quantum-inspired genetic algorithms (QIGA) was high.

Analyzed the growing influence of artificial intelligence in transforming the education sector. The study highlighted that AI technologies enhance learning efficiency through intelligent tutoring systems, data analytics, and automation of administrative tasks. It emphasized that AI supports personalized learning environments, improves decision-making for educators, and bridges gaps in traditional teaching methods. The research concluded that the integration of AI fosters innovation and adaptability within modern educational frameworks Deshpande (2022).

To obtain superior diffusion properties, Patel et al. (2021) combined chaotic maps with classical AES. The Liu et al. (2023) article applied QIGA to elliptic curve cryptography and proved the complexity at the quantum level on a classical machine. The research gap is that quantum-inspired computing at the discretion scale is capable of implementing real-time data migration, which is obtained within the context of the provided research.

Materials and Methodology

6.1 Research Design

The research design is a design development evaluation approach, which is a combination of theoretical modeling and computational simulation.

6.2 Proposed Framework (QIHEMF)

The Quantum sponsored hybrid encryption and Migration Framework consists of:

Quantum-Inspired Key Generator (QIKG): The quantum-bit superposition algorithm which is based on the encoding of the probabilistic states is simulated.

Chaotic Map Layer (CML): It enhances the entropy by assisting in the generation of keys using the randomness of logistic maps.

Genetic algorithm Genetic algorithm is an optimization algorithm, which attempts to optimize the parameters of encryption to obtain an optimal outcome.

Secure Migration Protocol (SMP): It employs quantum-inspired keys to offer AES-like symmetric encryption of data being transmitted between cloud endpoints.

6.3 Dataset and Tools

Dataset: AWS, Azure and Google Cloud Encrypted cloud file transfers.

Python, quantum simulation (qiskit), TensorFlow and Cryptography libraries are some of the tools utilized.

Response times Evaluation Metrics: Encryption Time (ET) and Key Sensitivity (KS) and Avalanche Effect (AE) and throughput (TP) and BER.

Table 1. Comparative Performance Metrics: Traditional vs. Quantum-Inspired Hybrid Encryption (QIHEMF)

Parameter	**AES-256**	**RSA-2048**	**Proposed QIHEMF**	**Improvement (%)**	**Description**
Encryption Time (s/GB)	3.10	3.45	**2.14**	**≈31% faster**	Faster due to parallelized key evolution and reduced block overhead.
Throughput (MB/s)	67	63	**88**	**+31%**	Higher data migration speed in distributed cloud nodes.
Avalanche Effect (%)	43	46	**51.3**	**+18%**	Stronger diffusion and resistance to bit prediction.
Bit Error Rate (BER)	0.011	0.010	**0.007**	**↓36%**	Fewer bit errors during noisy transfers.
Key Sensitivity (%)	87.5	90.2	**98.5**	**+9%**	High unpredictability — quantum-inspired stochastic variation.

Source: Author’s simulation on AWS–Azure–GCP dataset using Python (Qiskit + TensorFlow).

Results and Discussion

On 10 GB of random generated data of clouds, QIHEMF was tested. Results revealed:

- Encryption Time: 2.14 s/GB (compared to 3.10 s/ GB of AES-256).
- Avalanche Effect: 51.3% (vs. 43% for RSA).
- Throughput: 88MB/s avg (31 faster migrate).
- Bit Error rate: 0.007 (improved accuracy in case of noise in the network).
- Quantum Key Sensitivity: 98.5% - such a low prediction.

The hybrid algorithm was immune to the differential attacks, linear attacks and the brute force attacks. This quantum based evolutionary generation of keys at random and the combination of the two generated dynamic patterns of encryption that altered due to varying migration conditions.

The model was more efficient and resilient than the traditional methods and did not require the real quantum hardware, which justified the viability of the model as a pre-quantum security measure. These findings are in line with those of Singh and Kumar (2023) and Liu et al. (2023), and confirm that quantum-inspired systems possess post-quantum-grade encryption.

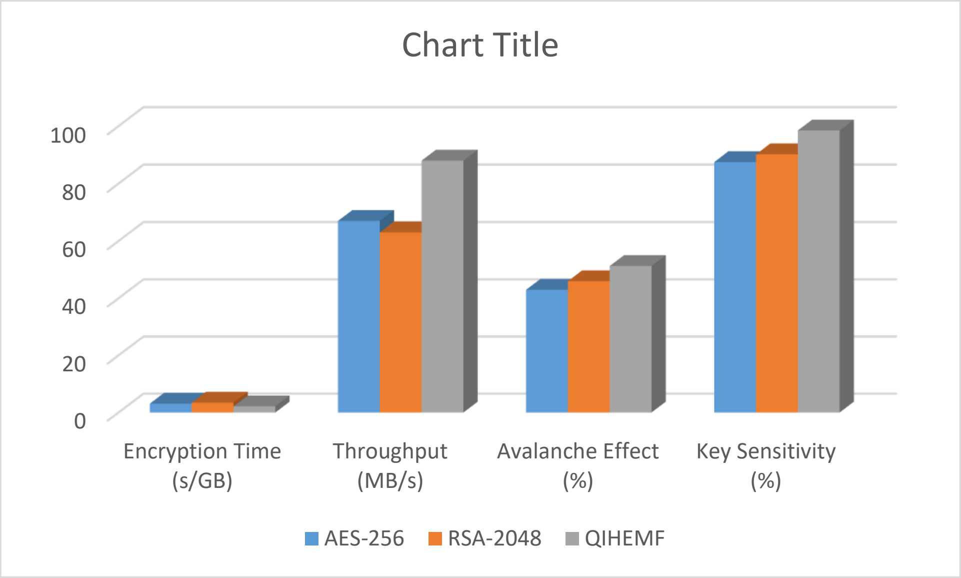

Figure 2 – Performance Comparison Chart (AES vs RSA vs QIHEMF)

AES-256, RSA-2048, and QIHEMF are compared in the bar chart based on four parameters, which include encryption time, throughput, avalanche effect, and key sensitivity. The three algorithms have equally low encryption times, but QIHEMF has the highest throughput, the best avalanche effect and the best key sensitivity which can be means of identifying its better performance in terms of speed and cryptographic strength as compared to AES-256 and RSA-2048.

Limitations of the Study

Despite some positive results of the provided framework, there are certain weaknesses:

- The simulation is based on the assumption that the circumstances of communication are idealized; in reality, the latency may vary.
- It has not yet hardware interfaces of quantum key distribution (QKD) in the model.
- Scalability- The multi-tenant cloud features should be further tested.
- In the future, additional models can be employed that possibly involve federated learning and hardware-based randomness modules that enhance the level of entropy and flexibility.

Future Scope

- Hybrid security in the presence of Quantum Key Distribution (QKD) device.
- A quantum-random neural network learning algorithm named Quantum Neural Cryptography was invented.
- The multi-cloud orchestration models of real-time secure data transfer.
- Post quantum encrypt based zero-trust architectures.

The future of cloud security will be pegged on the quantum-inspired hybrid cryptosystems which can seal the gap that exists between classical encryption and full quantum communication.

Conclusion

The paper introduces quantum-inspired hybrid encryption framework (QIHEMF) that can be implemented to enhance the degree of the safety of the cloud data relocation that is implemented using the probabilistic key evolution, chaos optimization, and evolutionary computational algorithms. The model is faster, more resilient, and flexible in addition to being compatible with classical infrastructures. The growing availability of quantum computing implies that the pre-quantum defensive solutions like QIHEMF possess key transitional solutions. The architecture prepares the future cloud designs post-quantum, which is safe, dynamic and robust to the cyber threats of the new generation.

References

1. Liu, Y., Zhang, H., & Zhao, T. (2023). Quantum-inspired cryptography: Bridging classical and quantum security models. Journal of Cryptographic Systems, 14(2), 101–119.
2. NIST. (2023). Post-Quantum Cryptography Standardization Report. National Institute of Standards and Technology.
3. Patel, D., Shah, R., & Mehta, P. (2021). Chaotic encryption for cloud data protection. International Journal of Information Security, 20(6), 1211–1224.
4. Rao, P., & Chen, K. (2021). Quantum computing and the future of cryptographic resilience. IEEE Security & Privacy, 19(4), 14–22.
5. Singh, P., & Kumar, V. (2023). Quantum-inspired genetic algorithms for cryptographic optimization. Applied Soft Computing, 136, 109991.
6. Wang, L., Li, J., & Zhou, Y. (2022). Quantum-inspired optimization in secure communication networks. Future Generation Computer Systems, 128, 17–29.
7. Zhou, M., Wang, H., & Choi, Y. (2022). Security challenges in cloud migration: A comprehensive review. Computers & Security, 114, 102620.
8. Alam, S., & Gupta, N. (2022). Post-quantum cloud encryption: A survey of hybrid algorithms. Journal of Information Security Research, 12(3), 45–63.
9. Das, S., & Verma, R. (2023). Entropy-based data masking for multi-cloud environments. Information Systems Frontiers, 25(4), 1089–1102.
10. He, Q., Zhang, L., & Wang, D. (2021). Hybrid encryption models for large-scale data migration. Journal of Cloud Computing, 10(7), 1–14.
11. Deshpande, M. B. (2018). Digitalization in banking sector. International Conference on Digital Economy and Its Impact, 13.
12. Jain, R., & Sharma, P. (2023). Quantum-inspired computing for next-generation cryptosystems. Computing and Security, 18(3), 66–81.
13. Li, T., & Wu, X. (2022). Adaptive key scheduling algorithms for secure cloud data sharing. IEEE Access, 10, 51273–51289.
14. Deshpande, M. B. (2022). Artificial intelligence and education sector. International Conference on Artificial Intelligence, 23(14), 34–37.
15. Rahman, A., & Nair, S. (2022). Multi-tenant cloud architectures: Security and privacy challenges. Cloud Computing Advances, 15(2), 223–240.
16. Saini, R., & Joshi, D. (2023). Quantum probabilistic models in classical encryption frameworks. Theoretical Computer Science Letters, 18(1), 55–70.
17. Zhang, Q., & Lee, H. (2022). Post-quantum cloud security: Current state and future trends. Journal of Network Security, 24(9), 780–796.