International Journal of Computational and Electronic Aspects in Engineering
Volume 5, Issue 4, December 2024, pp 214 - 228
https://doi.org/10.26706/ijceae.5.4.20241109

Quantum Cryptography-Enabled Cloud Security (QCECS) Framework

Wassan Adnan Hashim

Medical Instruments Techniques, Department, Al-Qalam University College, Kirkuk, Iraq
https://orcid.org/0000-0001-8473-8595

*Correspondence: wasan.eng@alqalam.edu.iq

Abstract: The QCECS Framework is ready to prevent new types of threats in the cloud environment given the increasing threat potential of quantum computing. RSA and ECC conventional encryption techniques cannot protect data security from quantum penetration and, therefore, the need for quantum security models. This incorporates the QKD for the impenetrable key exchange, post-quantum cryptography for data scrambling, blockchain for a more transparent way of managing keys, and the use of Artificial intelligence for real-time intrusion detection especially for traditional as well as quantum threats. At the same time, the proposed framework forms a symmetrical hybrid encryption approach with both quantum-resistant and classical interference to deliver the best outcomes while maintaining security integrity. The evidence derived from the study indicates that the framework protects the data through cryptographic mechanisms such as lattice-based cryptography and QKD and key management is secured through blockchain. It is crucial to mention, that the application of AI improves the detection of new threats in process and real time. This framework provides higher encryption strength, clarity, and quantum security compared to other methods. Even though various obstacles are resolved in the framework, several barriers remain in terms of hardware access, cloud adaptability, and internal enhancement. Yet, due to its novel approach to post-quantum cybersecurity, it has become a potential dominating solution for future cloud security.

Keywords: Quantum Key Distribution (QKD); Post-Quantum Cryptography; Blockchain-Based Key Management; Hybrid Encryption Models; AI-Driven Intrusion Detection.

Article – Peer Reviewed
Received: 05 October
Accepted: 02 Dec 2024
Published: 30 Dec 2024

Cite this article: Wassan Adnan Hashim, "Quantum Cryptography-Enabled Cloud Security (QCECS) Framework", *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 5, issue 4, pp. 214-228, 2024.
https://doi.org/10.26706/ijceae.5.4.20241109

1. Introduction

Cloud computing is a solutions-based processing model for data storage by availing a scalable, flexible and cost-effective infrastructure for organizations. However, with the increasing popularity of cloud environments for storage and management of personal data has also emerged criticism over security of such data. Past methods of data security like RSA and ECC (Elliptic Curve Cryptography) have been applied to secure data transfer as well as for storage in cloud systems[1, 2]. These methods are based on the computational difficulty in solving some mathematical problems including factoring of integers and discrete logarithms, for the intended protection of data. However, the reality today is that quantum computing, which is repeatedly predicted to disrupt the widely used cryptographic algorithms, is already on the horizon[3]. New technology such as quantum computers due to their capability to compute problems with higher numbers and exactitude can hack current encryption techniques placing data in clouds in danger. The consequence of creating an environment where quantum computing technology will be vital is that quantum-resistant security frameworks are becoming more relevant with every passing day. Such a change in the domain of cybersecurity has resulted in the emergence of innovative approaches, including Quantum Key Distribution (QKD), and post-quantum cryptographic algorithms, to ensure the adaptability of cloud security systems as shown in figure 1 [4].

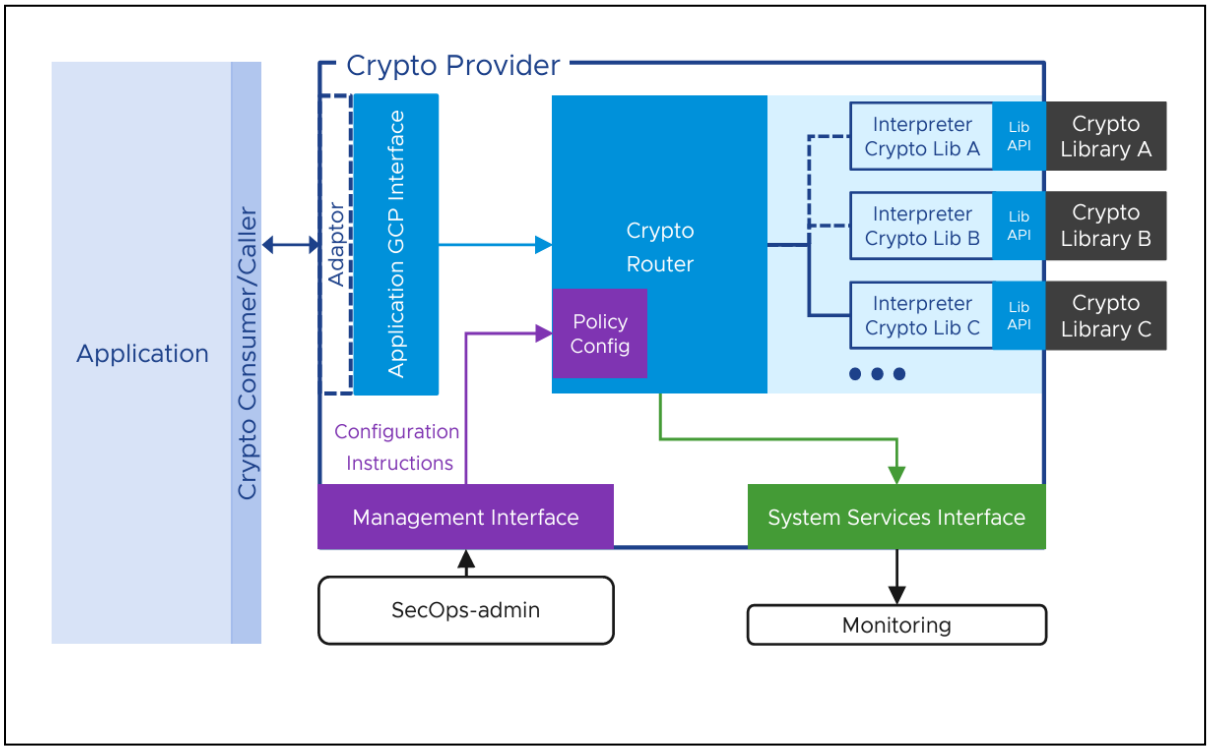

Figure 1. Generic Cryptographic Provider Functional Diagrams[4]

One of the major challenges that have informed the creation of a Quantum Cryptography-Enabled Cloud Security Framework is the emerging danger of attacks from Quantum Computing systems. Currently used cryptographic protocols which secure communication networks from the classical attacks fail against quantum attacks. This framework is inspired by the logic to protect cloud infrastructures in the post-quantum environment where both quantum and classical risks are inevitable. It is worth noting that authors of several works revealed that traditional encryption algorithms are easily susceptible to quantum attacks. Point out that cryptographers must be agile in terms of quantum-resistant algorithms when presenting the concept of post-quantum cryptography as the protective measure of the future IoT [4, 5]. The motivation also stems from the desire to achieve high levels of security while at the same time, the security

measures adopted should not have any negative impacts on the rate at which data is processed and transferred in the cloud service. The strengths of the paper propose viable solutions for the forthcoming quantum threats in the era of quantum computing. Its key contributions include:

- Quantum Key Distribution (QKD): Using the principles of quantum theory, the framework guarantees the secure exchange of encryption keys between the two parties. Using QKD, the eavesdropping of the key is certain to appear making the system safe.
- Post-Quantum Cryptographic Algorithms: To protect against future quantum attacks, the algorithms used in the framework are quantum-safe from both classical and quantum computing-based cryptanalysis. These algorithms give continued protection to the cloud data resources which could be very sensitive.
- Blockchain-Based Key Management: Key management is decentralized and technologies of blockchain to keep transparency and validation of cryptographic keys are used.
- Hybrid Encryption Models: Besides, the proposed framework makes better use of the quantum-resistant encryption approaches or classical ones depending on the type of data that is kept in the cloud environment.
- AI-Driven Intrusion Detection: AI is integrated into the framework for the concurrent identification and handling of security risks in real time. This makes it possible for an immediate detection of both classical and post-syntactic-based quantum attacks.

While the framework offers a promising solution to securing cloud environments in the quantum era, several challenges must be addressed:

- Quantum Hardware Availability: Quantum cryptography, like the QKD used for wide distribution, would not be possible without quantum communication equipment. At present, there are few implementations of quantum communications, and integrating quantum technology with large cloud networks is an insurmountable challenge.
- Integration with Existing Cloud Infrastructure: Most of the current cloud systems use classical encryption techniques, and, therefore, the switch to the quantum-resistant environment will entail major modifications to the hardware and software components. A keen challenge is backward compatibility and avoiding disruption of cloud services during this process of change.
- Performance Overheads: As for key post-quantum cryptography and quantum key management can cause increased latency and computational overheads. One of the major challenges that will be essential to address for the framework to be successful in realizing its goals will be the trade-off between security and performance; particularly in real-time applications.
- Regulatory and Compliance Issues: With the advancement in Quantum cryptography and post-quantum algorithms that are likely to be adopted into the Cloud security architectures there will arise emerging legal and regulatory issues on data privacy and protection, international standards governing the cloud solutions as well as management of Cryptographic key across geographical regions.

2. Literature Review

Among the most recent advances in technologies that have recreated the face of cybersecurity is quantum computing. RSA and Elliptic Curve Cryptography are some of the typical cryptographic methods in danger from quantum computers due to their high-speed capability to solve complex problems. This means that new cryptographic frameworks that are immune to quantum threats that present a threat to cloud, IoT and big data systems are needed. The following papers provide solutions from the field of post-quantum cryptography, application of blockchain, game theory, and hybrid cryptographic paradigm. These are pursued to protect data and application interconnects, data clouds, and IOT networks against traditional and new-generation threats such as quantum computing. In[1] consider Post-Quantum Cryptography (PQC) option for securing the IoT. To counter the attack from quantum computers, the authors have developed cryptographic methods based on lattice structures. In this case, the emphasis is on building PQC that would seamlessly fit into IoT ecosystems, so that data remains resistant to interception even as the quantum landscape evolves. Show how Quantum Key Distribution (QKD) can be employed in the process of encrypting the communication between cloud containers. Hence, through the usage of quantum networking channels, the paper presents an approach to safeguard distributed cloud infrastructure against both traditional and quantum-style cyber threats[2]. In [3] thesis presents a novel encryption framework to secure data integration in IoT using blockchain. The lightweight algorithm results in low latency and delivers high security for IoT data communication while working well in decentralized networks. A critical evaluation of Schiermeyer's work on Hessian elliptic curves for protocol security and privacy of applying ECC in securing communication systems. The authors mainly concentrate on identifying the opportunities and threats that the development of ECC offers and how this organization can create a post-quantity security mechanism by using cryptographic choices [4]. In [5], the Authors introduced a game theory-based approach to implementing a secure Internet of Vehicles (IoV) through blockchain. Advanced authentication between cars and structures is also maintained through the framework where data exchange is also done on blockchain. Paper[6] is devoted to the introduction of the subject of quantum information theory and contains material on entanglement, quantum teleportation and quantum error correction. This paper looks at how these concepts can be employed in the area of quantum cryptography and secure communication systems. In [7], the authors explore how neural networks can improve as well as jeopardize cryptographic systems. In the given study, the author also poses that neural networks are a double-edged sword in contemporary cybersecurity. The authors in [8] have developed a hybrid security model that combines features of adaptive learning with conventional cryptographic methods. This model will be capable of updating new threats in the big data environment and also enhance both the security as well as the real-time threat detection. This paper presents an overview of the most recent cybersecurity trends in the automotive industry; particularly on the application of blockchain and quantum cryptography for the protection of vehicular networks against cyber threats [9]. In [10] the topic of Cryptography and neural networks amounts of details about their relationship and possible collision are described. The authors discuss how the quantum system will improve the next cryptographic systems and the link between cryptographic systems and AI. In [11], the dual function of neural networks in cryptography is examined, highlighting its capacity to both compromise existing encryption and improve cryptographic methodologies. The document emphasizes the developing interplay between neural networks and cryptography, particularly in light of

advancements in AI and quantum computing. In [12], digital trade provisions in regional trade agreements (RTAs) between India and Asia-Pacific countries are discussed with a focus on how these provisions speak to cybersecurity, especially during crises such as the COVID-19 pandemic. In [13], the performance assessment of lightweight cryptographic algorithms more appropriate for constrained application spaces such as IoT is discussed. The author provides tangible upgrades to bolster and make them secure and faster in their execution of tasks. An advanced cryptographic framework for cloud computing systems is suggested, with an emphasis placed on implementing superior methods of scrambling information in the cloud [14]. Outlines major security issues related to big data and suggests several cryptographic solutions to improve security in the large-scale data context [15]. Explores the digital trade chapters incorporated in RTAs of India and Asia-Pacific nations to understand the changes they have undergone due to the crisis, including the COVID-19 pandemic. It focuses on security, privacy, and protection of data as being fundamentals of these arrangements [16]. The performance of different lightweight cryptographic algorithms, including IoT devices, was studied in [17] dissertation. It captures both the security aspect well as the optimization of these algorithms and suggests certain algorithms to be used in specific IoT and other analogous contexts. Presented an improved cryptographic model for cloud computing where data protection was a principal concern that was facilitated by improved cryptographic algorithms. The paper describes the weaknesses in cloud technologies and proposes how the data can be protected both while transferring and while stored [18]. In [19] the author identifies the most significant security issues inherent in big data: data leakage, privacy, and cyber threats. To address such issues, the authors suggest several cryptographic solutions to improve the assurance of data protection in big data systems. In [20] describes a cloud security model that makes use of the Okamoto-Uchiyama model of cryptography, which is under the public key cryptographic model. It means that the concern is more on protecting cloud structures, more enhanced encryption mechanisms and ensuring that only authorized individuals gain access to cloud information, the proposed model shown in Figure 2.

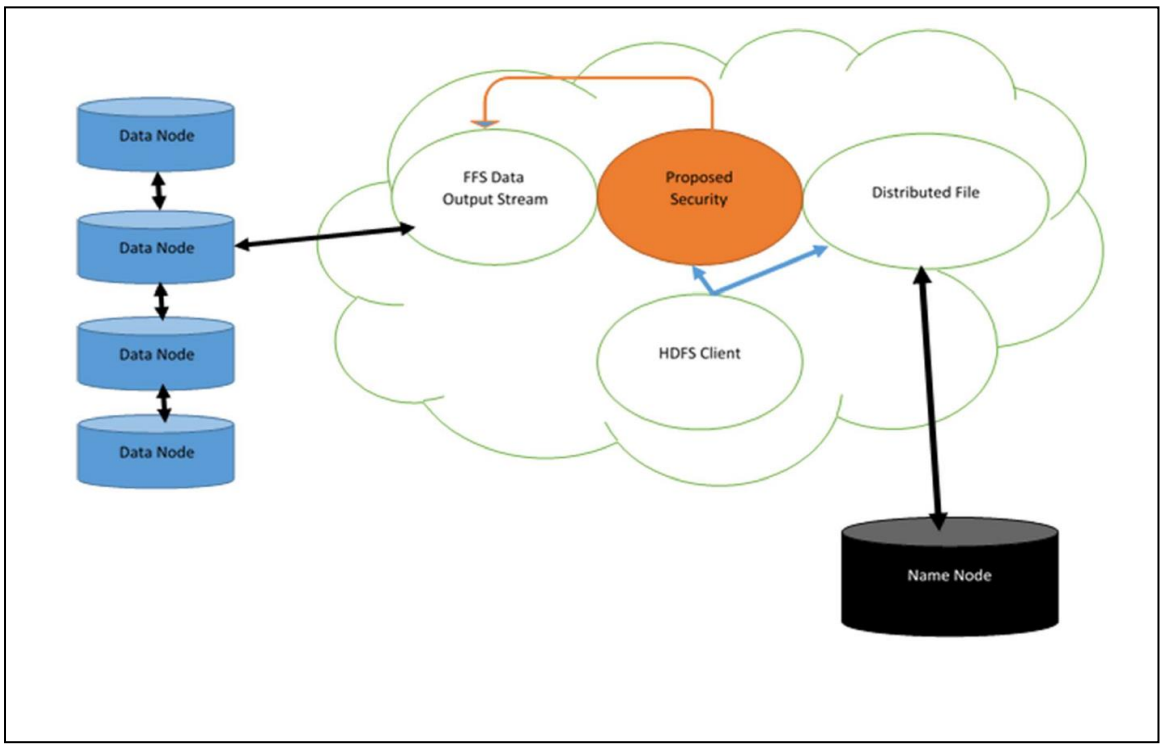

Figure 2. Encryption and Decryption procedure in HADOOP[20]

In [21] the authors put forward a guideline for encryption of big data using the integration of Paillier and RSA cryptography with a view of making big data security strong. Caution is given to bring out the key factors that would enhance not only the encryption strength but also the efficiency of secure information transmission in large-scale data systems. This paper will discuss a framework of using a method Integrating cryptographic algorithms to protect data on cloud service providers. The authors also put forward a system for the protection of data that are stored and in transmitted formats that safeguard the privacy and security of cloud users [22]. Explains how identity-based cryptography can be used to improve security in the cloud. For instance, the authors suggest that cryptographic keys should be created based on user

identities, which will enhance the key management system in cloud environments[23]. A framework for cryptographic security that incorporates cloud networks with IoT networks was suggested. The nature of the presented hybrid framework is to protect communications and data transfer between IoT devices and cloud platforms due to the specific conditions under which their combination occurs [24]. Proposes a scheme known as fuzzy-based cryptography to enhance Cloud security system. The method enables the protection of data in the cloud because fuzzy logic improves encryption processes in the framework to make it elastic in overcoming threats[25]. In [26] The authors put forward a cybersecurity model for data transfer and storage within cloud contexts through cloud cryptography. The model fulfils the existing demand for specific encryption algorithms that ensure the confidentiality of transmitting data and block unauthorized data access. Improved version of the AES (Advanced Encryption Standard) algorithm to improve security for cloud computing. The authors describe modifications of the AES that would make it more immune to other modern threats to cyber security and therefore keep cloud data safe [27]. In [28] a biometric authentication and image encryption system for image protection in the cloud is proposed. To provide safe cloud image storage and transfer solutions, the authors integrate human biometric data with encryption methods. Investigate emerging cryptography innovations intended to improve the protection of cloud computing. The authors propose several works that offer high protection levels along with high performance, thus offering cloud platforms more efficient encryption methods [29]. In [30] looks at the issue of secure cloud storage looking at solutions that use cryptographic methods to secure data stored on the Cloud.

The authors suggest how the security of stored data in cloud systems can be improved through proper encryption methods and protocols. In [31] study proposes SecCaos-Image, a new symmetric encryption algorithm to enhance the reliable and safe transmission of the image. key schedule generation is done by adopting the logistic map and Lorenz equations hence exhibiting efficiency of high entropy and poor correlation in the processed encrypted images. The proofs show that the algorithm is resistant to cryptanalysis and more useful in medicine and finance, where data accuracy is important. In the paper [32], the authors establish a trust model for Cloud Data service providers and key factors are Security, Cost, Disaster Recovery, Authentication. With reference to a multivariate logistic regression analysis, the authors analyse the user perspective on trust in context to cloud services. COVID-19 is highlighted as a key factor in the expansion of cloud solutions in the course of the study, and a set of proposals for enhancing credibility of cloud services is provided. A new wide-ranging study delves into several measures to prevent computer malware attacks and compared tools and approaches like machine learning, deep learning and dynamic analysis. The study classifies the malware types, points out the drawbacks of the traditional approach to antivirus techniques, and presents new detection techniques including API sequence analysis. The study also portrays how the emerging threats such as polymorphic and metamorphic malware require usage of versatile approaches [33]. In [34] evaluates the applicability of cloud computing as a method of handling big data for the virtual library of the University of Mosul. In this case, the study provides the following opportunities to the adoption of cloud computing; cost reduction, scalability, and accessibility to cloud services, whereas the challenges include; limitations with infrastructure and talent acquisition. Therefore, the results imply that cloud implementations are necessary for future advancements in academic library systems. In [35], a secure electronic payment system was developed using the Kerberos cryptographic protocol to include both authentication and encryption aspects for the improvement of transaction security. By using ticket-granting mechanisms, the system achieves privacy and data/procedure integrity and at the same time it is computationally inexpensive. Mobile banking and e-commerce applications are the particular focus of the presented paper that proves the system's safety and convenience.

3. Methodology

The proposed Quantum Cryptography-Enabled Cloud Security framework focuses on preventing data and cloud resources hacking by using Quantum cryptography, post-quantum cryptographic algorithms, using Blockchain-based key management system, and advanced AI-based IDS. Figure 3 shows the proposed model, also breakdown of each step, as well as how the framework is constructed and how each component defends cloud architecture from classical and quantum-security-based threats.

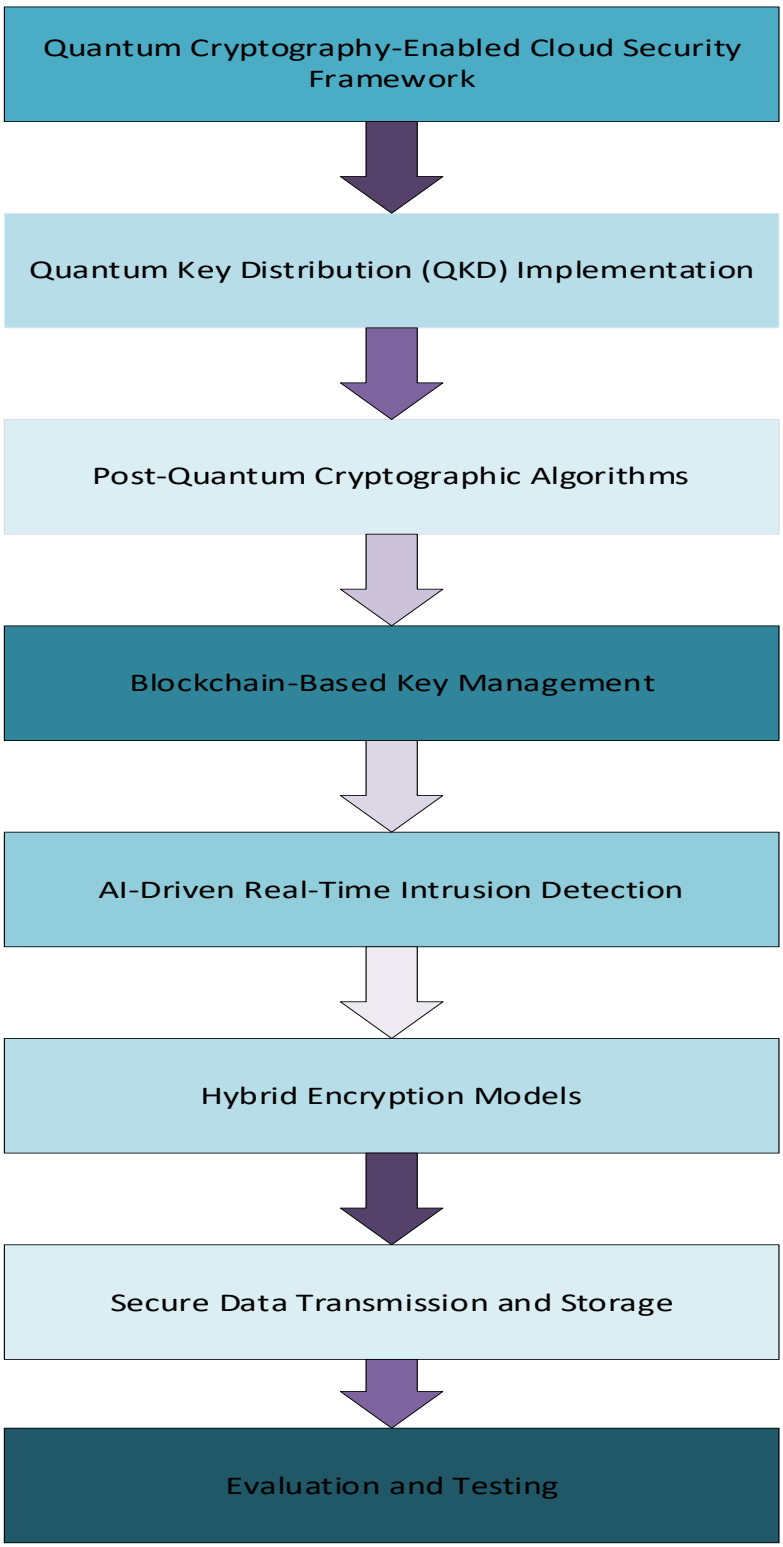

Figure 3. block diagram of the proposed model.

A. Implementation of Quantum Key Distribution

Ensure secure key exchange between cloud user cloud and service provider using the principles of quantum cryptography to resist both eavesdropping and quantum attacks.

- Quantum Channel Setup: A separate quantum communication channel is formed for two actors. Here, data is conveyed as quantum bits or simply known as qubits. This is possible by using QKD protocols BB84 to ensure if anyone tries to intercept the key; it will be detected. This ensures that communication via the classical channel is secure even if the classical channel has been susceptible to tapping by an intruder.
- Qubit Transmission: They are quantum algorithms that use qubits, which is the encryption key, for transmission between two communicating parties. The process of quantum key exchange ensures the user that any attempt of eavesdropping will be detected by facts and principles that quantum mechanics has postulated that observing a quantum state changes its state, thus providing the key exchange a very high level of security.
- Measurement and Key Agreement: During transmission, the quantum information from the sender's party is transmitted to the receiver's party and then the parties make quantum measurements to get the key. Then apply quantum measure to compare portions of the key so that it matches with the other's key. Reconciliation if there are any differences involves the rejection of a compromised key.
- Key Validation: Since the keys being exchanged are public, the two parties will over a classical channel share a subset of the key to ensure that the keys are the same. If there are no measure errors, the remaining part of the key is used for encryption. This ensures that the key is changed reciprocally to ensure a secure connection between the client machine and the host machine.
- Key Integration: The validated quantum key is then used for symmetric encryption which in general is combined with algorithms such as AES (Advanced Encryption Standard) used to encrypt the transferred data in the cloud environment.

QKD makes communication secure and it is hard to hack because QKD works on principles of quantum mechanics. Whenever an attempt is made to listen into a particular link, the systems kill the current quantum states meaning that keys can only be accepted if they are proven to be safe.

B. EETF – Post-Quantum Cryptographic Algorithms

Use cryptographic algorithms that stand a good defence against attacks that will be enacted by quantum computers in the future to make the systems secure from both classical and quantum attackers.

- Algorithm Selection: In implementing a quantum cloud system, advanced cryptographic solutions are included, for instance, lattice-based (NTRU), hash-based, and code-based (McEliece). These algorithms are again immune to quantum algorithms like Shor's algorithm which is used for attacking traditional cryptographic algorithms such as RSA and ECC.
- Encryption and Decryption Process: The selected post-quantum algorithms are used for encrypting data both in transit and when stored in a database. For instance, lattice-based encryption can be employed in encrypting data during its transfer from one user to cloud providers while hash-based signatures can be employed in authenticating documents and communication.
- Key Exchange Protocols: Post-quantum key transit algorithms including Kyber are used to exchange cryptographic keys even when the adversary has a quantum computing capability. These protocols assure that classical as well as quantum-safe symmetric keys can be exchanged.
- Hybrid Encryption Implementation: Since the new system should be compatible with the existing systems, a composite encryption model is used incorporating post-quantum and classical cryptographic techniques. This makes it possible to shift to fully quantum-resistant solutions step by step while degrading today's services.

While building a new era of quantum computing, post-quantum algorithms are a critical solution for keeping encrypted information safe and protecting it against future quantum threats. The ability to integrate methods that will provide future protection against quantum attacks makes the current method quite efficient without compromising on subsequent enhancements.

C. Blockchain Based Key Management

Apply blockchain to decentralize and to substantially safeguard cryptographic keys from unauthorized access to maximize their usage's openness and immutability.

- Blockchain Ledger Creation: A blockchain is employed to record and control the flow of cryptographic keys. All the management operations (generation, distribution and revocation) of keys are noted in the blockchain and due to this, it is almost impossible to alter the records of these operations.
- Smart Contracts for Key Management: This paper further establishes smart contracts to drive key generation, dissemination, validation, and revocation. For instance, these contracts run on their own as soon as certain conditions are met so as to ensure that proper cryptographic policies are adopted.
- Distributed Key Storage: The data itself is distributed among the multiple nodes within the blockchain network where individual user identities do not have exclusive rights to all keys. This cuts the risk of key compromise due to insider attacks or the presence of central points of failure.
- Key Validation and Auditing: Every key is checked against the consensus mechanism of the blockchain to check if it has been tampered with or not. There is clear visibility in key management, and the blockchain serves the purpose of an audit trail to meet regulatory and legal compliance to support forensic investigation.
- Blockchain helps in maintaining transparency and has permanency of records which makes key management safe without the intervention of an authority. The decentralized way enhances security and; smart contracts are effective in enforcing other lifecycle policies.

D. Real-Time Intrusion Detection Through Artificial Intelligence

Implements Artificial Intelligence to protect from security breaches and attacks and recognize classical and quantum attacks.

- Data Collection for Training: Data in cloud environments include baseline logs, activity patterns and past attack information. This data is then utilized in training Artificial Intelligence in identifying inadmissibility or even threats.
- Machine Learning Models for Threat Detection: This includes real-time behavioral analysis, through Convolutional Neural Networks (CNNs) or Recurrent Neural Networks (RNNs) to learn if the observed behavior is malicious or if it follows an abnormal pattern. Such models can identify many abnormal signals that might not be identified by other more traditional means.
- Threat Classification and Response: Depending on what has been learnt through training, the AI models differentiate between various types of threats including data breaches, quantum attacks, and insider threats. Depending on the classification made, automated remedial actions are initiated (for example; quarantining the involved server, de-authorization of keys or emailing the administrators).
- Continuous Learning and Adaptation: The AI models are always improving over time depending on new threats that are being encountered in the market. What is important is the usage of reinforcement learning or unsupervised learning to enhance the ability of the models to identify new forms of attacks, including quantum-based ones.
- AI-based platforms are proactive and optimal defence, this way an attack can be easily counteracted as the AI predicts it. Such is possible due to the machine learning approach that enables large and fast MP graph changes in response to new and emerging threats, including Quantum Adversaries.

E. Hybrid Encryption Models

Integrate QR and CE to have a more effective and efficient result between security and performance.

- Layered Encryption Design: AES uses in symmetric key encryption are integrated with post-quantum cryptographic usage. Structured data in an organization that requires protection and has strict security requirements, is protected by post-quantum cryptography while other data that does not need heightened security is protected by classical cryptography, as they offer better performance.
- Key Management for Hybrid Encryption: It means that classical and post-quantum keys for cryptographic purposes are under the control and administration of the blockchain system. Depending on the kind of data, it is either sensitive, different keys and algorithms are used in the process of encryption and decryption.
- Gradual Transition Plan: An integrated paradigm enables a transition to post-quantum cryptosystems as a shift of key-exchange algorithms can be made gradually. Afterwards, as the quantum-resistant systems spread around the globe, the classical algorithms can then be halted.

- Hybrid encryption provides the best of both worlds: protection from future quantum advanced attacks without the decline in the current system's efficiency. It enables a smooth and disruptive transition to quantum-resistant security as well as an optimized trade-off between key length and computation costs.

F. To Ensure Secure Data Transmission and Storage the Following Key Factors Have to Be Enacted.

Make sure that data assets are protected during upload and storage, in the quantum and conventional cloud setting.

- Quantum-Resistant Communication Channels: Introduce QKD-secured and post-quantum encrypted control connections for all the communication between the cloud users and service providers.
- Data Encryption Before Transmission: Every data transferred within the cloud network uses a hybrid encryption model to facilitate secure data transfer. Some data is encrypted as sensitive data using post-quantum encryption and other data is encrypted as normal data using traditional encryption.
- Secure Cloud Storage: Information maintained in the cloud is secured by employing post-quantum cryptography so to ensure perfection even in the future. To safeguard the data, techniques such as encrypted file systems and secure access protocols against classical and quantum adversarial frameworks are applied.
- The framework also guarantees that data is protected from future quantum threats and at the same time ensures proper performance of the current cloud processes with data encrypted both in transit and at rest quantum-resistant methods.

G. Evaluation and Testing

Assess the stability and reliability of the framework in scenarios and assess its strengths and vulnerabilities in a virtual setting.

- Simulated Quantum Attacks: Conduct virtual quantum attacks via adopted quantum algorithms such as Shor's algorithm to conform to the efficiency of the post-quantum cryptographic algorithms besides the QKD system.
- Benchmark Performance: Determine the amount of delay time, and volumes of traffic processed in the cloud infrastructure for quantum-resistant algorithms. Compare the performance of classical and hybrid encryption models, to enable infrastructure designers to avoid negative impacts that subsequently affect cloud services.
- Security Audits: Conduct regular security audits to verify the proper implementation of cryptographic protocols, key management, and AI-driven detection systems. This ensures that the framework operates as intended in real-world scenarios.
- Comprehensive testing ensures that the framework is secure against quantum threats and operates efficiently in real-world environments. Simulations of quantum attacks validate the effectiveness of the quantum-resistant technologies integrated into the system.

4. Result and Analysis

A financial institution, "QuantumBank," is moving its transaction processing system to a cloud infrastructure. The bank deals with millions of sensitive financial transactions daily, requiring encryption for secure communication. However, with the anticipated advent of quantum computers, traditional encryption methods such as RSA and ECC are no longer considered secure. QuantumBank is implementing the Quantum Cryptography-Enabled Cloud Security Framework to safeguard transactions against both classical and quantum-based threats. To illustrate how the Quantum Cryptography-Enabled Cloud Security Framework secures financial transactions using Quantum Key Distribution (QKD) and Post-Quantum Cryptographic Algorithms by providing a mathematical example for key exchange and encryption. The procedure of the proposed model is shown in figure 4, below are Step-by-step mathematical scenario for the proposed model.

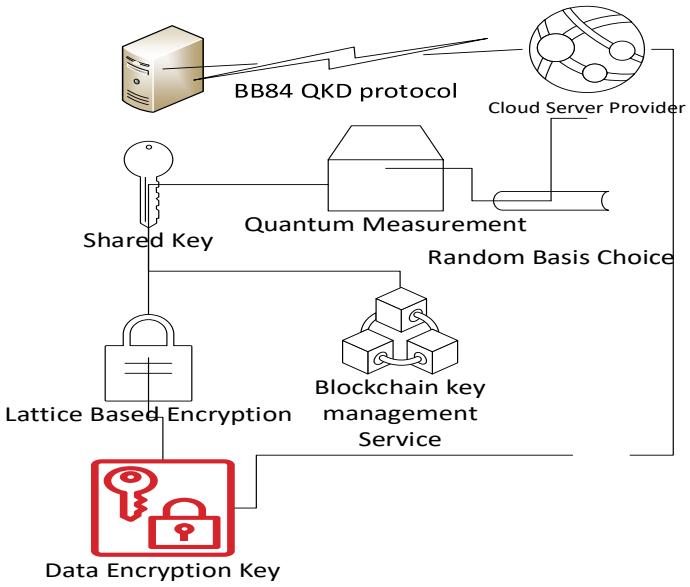

Figure 4. procedure of the Proposed model

A. Quantum Key Distribution (QKD) Setup

Quantum Bank wants to securely exchange encryption keys between its main server and the cloud service provider using QKD (BB84 protocol). The key exchange process involves encoding the key in qubits, which are transmitted over a quantum channel.

Let's assume they are trying to exchange a 4-bit encryption key.

- **QuantumBit Transmission**: The bank transmits qubits using the BB84 protocol. The qubits can be in one of four possible states:
  - $|0\rangle$ (horizontal polarization),
  - $|1\rangle$ (vertical polarization),
  - $|+\rangle$ (45° polarization),
  - $|-\rangle$ (135° polarization).

Let's say the bank transmits the following qubits to the cloud provider:

Qubits Transmitted=$|0\rangle,|+\rangle,|1\rangle,|+\rangle$

- **Receiver's Random Basis Choice**: The cloud provider measures the qubits using a random basis (rectilinear or diagonal basis).
- **Measurement**: The cloud provider measures the qubits based on its chosen basis. If the basis matches the sender's, the qubit measurement will be correct. Otherwise, the measurement will result in a random value. Afterwards, both parties compare a subset of their basis choices over a classical channel to detect any eavesdropping attempts.

For matching results are: Measured Key=0,?,1,?

The mismatches are discarded, and the remaining bits (0, 1) are used as part of the encryption key.

Final Key: QuantumBank and the cloud provider now share a **2-bit key**: Shared Key=01.

This shared key is secure, as any eavesdropping would have been detected due to the nature of quantum measurement.

B. Post-Quantum Cryptographic Algorithms for Encryption

Once the QKD has provided a secure key, QuantumBank uses a post-quantum cryptographic algorithm (e.g., lattice-based cryptography) to encrypt a financial transaction message. Let's assume they want to encrypt the message "$1000 transfer."

Lattice-Based Encryption: In lattice-based cryptography, encryption involves embedding the message into a high-dimensional lattice and then performing operations on this lattice structure.

Let's represent the plaintext message "1000 transfer" as a vector **m** in a 2-dimensional lattice: $m = \begin{pmatrix} 1000 \\ 12345 \end{pmatrix}$, A random vector **r** is selected to obscure the message: r= $\begin{pmatrix} 3 \\ 5 \end{pmatrix}$

The lattice-based encryption algorithm generates a matrix A (known to both sender and receiver) and computes the ciphertext c as (c=A·m+r). For simplicity, assume the matrix A is: A= $\begin{pmatrix}21\\13\end{pmatrix}$, Performing the multiplication:

A·m= $\begin{pmatrix}21\\13\end{pmatrix}\cdot\begin{pmatrix}1000\\12345\end{pmatrix}=\begin{pmatrix}25345\\49035\end{pmatrix}$

Adding the random vector **r** to the result:

$\begin{pmatrix}25345\\49035\end{pmatrix}+\begin{pmatrix}3\\5\end{pmatrix}=\begin{pmatrix}25348\\49040\end{pmatrix}$

Ciphertext:

The encrypted message sent to the cloud provider is:

c=$\begin{pmatrix}25348\\49040\end{pmatrix}$

Decryption:

The cloud provider, knowing the matrix **A** and the shared key, can decrypt the message by reversing the process, subtracting the random vector, and solving for **m** using the lattice structure.

First, subtract **r** from the ciphertext:

c−r= $\begin{pmatrix}25348\\49040\end{pmatrix}-\begin{pmatrix}3\\5\end{pmatrix}=\begin{pmatrix}25345\\49035\end{pmatrix}$

Then, solve the linear system **A · m = (25345, 49035)** to recover the original message **m**.

The result will give:

$m=\begin{pmatrix}1000\\12345\end{pmatrix}$ This corresponds to the decrypted message: "$1000 transfer."

C. Blockchain-Based Key Management

QuantumBank records all key exchanges and encryption operations using blockchain-based key management. Each transaction involving encryption key generation and usage is logged in an immutable blockchain ledger for future auditing and security purposes. This ensures that even if an adversary attempts to tamper with the keys, the integrity of the cryptographic system is preserved, and all key exchanges are verifiable.

In this mathematical scenario, QuantumBank successfully used Quantum Key Distribution (QKD) to exchange secure encryption keys and leveraged lattice-based post-quantum cryptography to encrypt financial transactions securely. By integrating blockchain-based key management, the bank ensured transparency and audibility of key usage, creating a robust, future-proof encryption system that resists both classical and quantum computing threats. This framework ensures that sensitive financial data is protected against quantum attacks, making it highly secure for long-term cloud deployments in the finance industry.

Table 1. comparative of the proposed model with related work

Aspect	**Proposed Quantum Cryptography-Enabled Cloud Security Framework**	**Reference [1]: NTRUEncrypt for Big Data Security**	**Reference [5]: Post-Quantum Cryptography for IoT**	**Reference [6]: Quantum Networking for Cloud Security**	**Reference [18]: Hybrid Cryptography for Cloud**
Encryption Strength	Achieved robust encryption strength using post-quantum cryptographic algorithms like lattice-based cryptography and hybrid models. Resistant to both classical and quantum attacks.	Achieved quantum-resistant encryption using NTRUEncrypt, effective for large data sets but lacks hybrid encryption.	Achieved post-quantum encryption, effective for IoT environments, but without hybrid or layered encryption.	Achieved moderate encryption security through quantum networking, but lacks post-quantum algorithm integration.	Achieved encryption strength using classical algorithms (RSA + Paillier), vulnerable to quantum attacks.
Key Exchange Security	Achieved unbreakable key exchange with QKD (BB84	Secured key exchange through NTRUEncrypt, resistant to	Achieved secure key exchange for IoT environments using post-quantum	Secured communication through quantum networking but	Key exchange achieved through classical cryptographic

	protocol), providing real-time detection of eavesdropping.	quantum attacks but lacks the additional protection of QKD.	cryptography, but lacks QKD implementation.	without full-fledged QKD, making key exchange less secure.	methods, which are vulnerable to quantum decryption.
Key Management Transparency	Achieved full transparency and security in key management using blockchain, ensuring tamper-proof operations with smart contracts.	No blockchain implementation, limited transparency and control over key management.	No blockchain-based key management, relying on classical centralized methods.	Lacks blockchain key management, focusing more on communication security than key management transparency.	Achieved basic key management through centralized control, vulnerable to single points of failure and insider threats.
Intrusion Detection	Achieved real-time, AI-driven detection of both classical and quantum-based threats, significantly enhancing response time.	No real-time AI-driven intrusion detection.	No AI-based intrusion detection, only focuses on cryptographic protection.	No AI-based detection, primarily focused on secure communication.	No AI-driven intrusion detection, only relying on cryptographic methods.
Performance and Efficiency	Achieved a balance between strong quantum-resistant security and performance using hybrid encryption models, minimizing overhead.	Achieved efficiency with NTRUEncrypt, but lacks hybrid encryption to optimize performance further.	Achieved good efficiency for IoT applications with quantum-resistant algorithms but no performance optimization.	Achieved moderate efficiency through quantum networking but lacks hybrid models for optimizing performance.	Achieved good performance with classical algorithms but lacks the ability to resist future quantum threats.
Quantum Resistance	Achieved comprehensive quantum resistance using QKD, post-quantum cryptography, and hybrid encryption techniques, making it future-proof.	Achieved quantum resistance with NTRUEncrypt but lacks the integration of hybrid methods and QKD.	Achieved partial quantum resistance with post-quantum cryptography but no hybrid encryption or blockchain.	Achieved limited quantum resistance with quantum networking but no post-quantum cryptographic integration.	Lacks quantum resistance; fully vulnerable to quantum computing-based attacks due to reliance on classical cryptography.

The comparison and Achieved Results can be summarized as below:

1. Encryption Strength: The proposed model achieves strong encryption by combining post-quantum cryptographic algorithms (such as lattice-based cryptography) and hybrid encryption methods. This approach ensures that it is secure against both classical and quantum-based attacks. Other works, such as Ref [1] and Ref [5], offer quantum-resistant encryption, but without the flexibility or performance benefits of hybrid models. Reference [18] relies on classical methods, leaving it vulnerable to quantum decryption.
2. Key Exchange Security: The proposed model's implementation of Quantum Key Distribution (QKD) ensures unbreakable key exchange with real-time detection of eavesdropping attempts. None of the other references, including Ref [1], implement QKD, making their key exchange security less robust. Ref [6] does explore quantum networking, but lacks the security guarantees provided by a full QKD implementation.
3. Key Management Transparency: The proposed model uses blockchain-based key management, which provides decentralization, immutability, and transparency. This is a major advantage over other references like Reference [1], which rely on traditional key management methods that are more prone to central points of failure and insider threats.

4. Intrusion Detection: The proposed model achieves real-time AI-driven intrusion detection, capable of identifying both classical and quantum attacks, providing a significant advantage in threat detection and response time. This feature is absent in the compared works, such as Reference [1] and Reference [5], which focus purely on encryption without integrating AI for intrusion detection.
5. Performance and Efficiency: By employing hybrid encryption models, the proposed framework balances performance and security, ensuring minimal overhead while maintaining strong encryption. Reference [1] and Reference [5] achieve quantum resistance but do not focus on optimizing performance with hybrid techniques. Reference [18] provides good performance but is entirely vulnerable to quantum threats.

5. Conclusion

The Quantum Cryptography-Enabled Cloud Security Framework provides a comprehensive and future-proof solution to address the pressing cybersecurity challenges posed by the advent of quantum computing. By integrating Quantum Key Distribution (QKD), post-quantum cryptographic algorithms, blockchain-based key management, and AI-driven real-time intrusion detection, this framework ensures robust protection against both classical and quantum-based cyber threats. Its ability to combine quantum-resistant encryption with classical methods through hybrid encryption models allows for optimal performance without compromising security. The framework stands out from existing works due to its use of QKD, which guarantees secure key exchange by leveraging the principles of quantum mechanics. Additionally, blockchain-based key management ensures transparency and immutability, making the framework resilient to insider threats and offering verifiable key operations through smart contracts. AI-driven intrusion detection further enhances security by providing real-time detection of evolving threats, adapting to both classical and quantum-based attacks. However, while the proposed framework offers an advanced solution, certain challenges such as quantum hardware availability, integration with existing cloud infrastructures, and performance overheads associated with post-quantum algorithms must be addressed for full-scale deployment. Despite these hurdles, the framework offers a scalable and adaptable approach, making it a valuable model for securing cloud environments in the emerging quantum era. Its combination of cutting-edge cryptographic techniques, real-time threat detection, and decentralized key management positions it as a leading framework in the field of post-quantum cybersecurity.

References

[1] M. K. Yousif, Z. E. Dallalbashi, and S. W. Kareem, “Information security for big data using the NTRUEncrypt method,” *Measurement: Sensors*, vol. 27, p. 100738, 2023.

[2] G. Y. Ismail, S. Alhayali, S. W. Kareem, and Z. S. Hussain, “Secure Data in the Cloud with a Robust Hybrid Cryptographic Approach,” *Journal of Electrical Systems*, vol. 20, no. 2, pp. 2450–2457, 2024.

[3] S. M. J. Abdalwahid, B. F. Ibrahim, S. H. Ismael, and S. W. Kareem, “A New Efficient Method for Information Security in Hadoop,” *Qalaai Zanist Journal*, vol. 7, no. 2, pp. 1115–1138, 2022.

[4] D. Sikeridis *et al.*, “ELCA: Introducing Enterprise-level Cryptographic Agility for a Post-Quantum Era,” *Cryptology ePrint Archive*, 2023.

[5] A. Kumar, C. Ottaviani, S. S. Gill, and R. Buyya, “Securing the future internet of things with post-quantum cryptography,” *Security and Privacy*, vol. 5, no. 2, p. e200, 2022.

[6] B. Kelley, J. J. Prevost, P. Rad, and A. Fatima, “Securing cloud containers using quantum networking channels,” in *2016 IEEE International Conference on Smart Cloud (SmartCloud)*, 2016, pp. 103–111.

[7] M. Siddireddy, “A lightweight end-to-end encryption algorithm for IoT data integration: Blockchain framework.” Southern Illinois University at Carbondale, 2024.

[8] N. Purohit, S. Joshi, M. Pande, and S. Lincke, “Pragmatic analysis of ECC based security models from an empirical perspective,” *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 3, pp. 739–758, 2023.

[9] M. Gupta *et al.*, “Game theory-based authentication framework to secure internet of vehicles with blockchain,” *Sensors*, vol. 22, no. 14, p. 5119, 2022.

[10] R. Pandey, “Quantum Information Theory-Principles and Concepts: Exploring the principles and concepts of quantum information theory, including quantum entanglement, teleportation, and quantum error correction,” *Australian Journal of Machine Learning Research & Applications*, vol. 4, no. 1, pp. 240–248, 2024.

[11] B. Zolfaghari and T. Koshiba, “The dichotomy of neural networks and cryptography: war and peace,” *Applied System Innovation*, vol. 5, no. 4, p. 61, 2022.

[12] S. M. Sasubilli, A. K. Dubey, and A. Kumar, "Hybrid security analysis based on intelligent adaptive learning in Big Data," in *2020 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, 2020, pp. 1–5.

[13] C. P. Eze, J. Emmanuel, C. I.-O. Onietan, I. Isewon, and J. Oyelade, "Systematic Review on the Recent Trends of Cybersecurity in Automobile Industry," in *2023 International Conference on Science, Engineering and Business for Sustainable Development Goals (SEB-SDG)*, 2023, vol. 1, pp. 1–7.

[14] B. Zolfaghari, H. Nemati, N. Yanai, and K. Bibak, "The Dichotomy of Crypto and NN: War and Peace," in *Crypto and AI: From Coevolution to Quantum Revolution*, Springer, 2023, pp. 15–39.

[15] M. R. Naaz and A. Kumar, "Simulation Of A Secure Approach Of Data Communication On Peer To Peer Network Using Blockhain Technology On Ethereum," *Simulation*, vol. 18, no. 2, 2023.

[16] M. N. Rahman and N. Rahman, "Exploring digital trade provisions in Regional Trade Agreements (RTAs) in times of crisis: India and Asia-Pacific countries," *Asia and the Global Economy*, vol. 2, no. 2, p. 100036, 2022.

[17] S. Manjunath, "Experimental Evaluation of Lightweight Cryptographic Algorithms." BMS College of Engineering, 2022.

[18] M. Sudha and M. Monica, "Enhanced security framework to ensure data security in cloud computing using cryptography," *Advances in Computer Science and its Applications*, vol. 1, no. 1, pp. 32–37, 2012.

[19] S. Kareem, A. Hasan, R. Hawezi, K. Muheden, and F. Khoshaba, "Big Data Security Issues and Challenges.," *Journal of Applied Computer Science & Mathematics*, vol. 15, no. 32, 2021.

[20] S. W. KAREEM, "Secure Cloud Approach Based on Okamoto-Uchiyama Cryptosystem.," *Journal of Applied Computer Science & Mathematics*, vol. 14, no. 29, 2020.

[21] S. M. J. Abdalwahid, R. Z. Yousif, and S. W. Kareem, "Enhancing approach using hybrid pailler and RSA for information security in bigdata," *Applied Computer Science*, vol. 15, no. 4, pp. 63–74, 2019.

[22] M. Alrashidi and M. Alrashidi, "A Framework and Cryptography Algorithm for Protecting Sensitive Data on Cloud Service Providers," *journal of King Abdulaziz University Computing and Information Technology Sciences*, vol. 8, no. 2, pp. 69–92, 2019.

[23] H. Li, Y. Dai, and B. Yang, "Identity-based cryptography for cloud security," *Cryptology ePrint Archive*, 2011.

[24] S. Farooq, P. Chawla, and N. Kumar, "A cryptographic security framework for hybrid Cloud-Internet of Things network," *Security and Privacy*, vol. 6, no. 5, p. e309, 2023.

[25] P. Kanagala and R. Jayaraman, "Effective encryption approach to improving the secure cloud framework through fuzzy-based encrypted cryptography," *Soft Computing*, pp. 1–10, 2023.

[26] H. Dubey, S. Kumar, and A. Chhabra, "Cyber security model to secure data transmission using cloud cryptography," *Cyber Secur. Insights Mag*, vol. 2, pp. 9–12, 2022.

[27] I. A. Awan, M. Shiraz, M. U. Hashmi, Q. Shaheen, R. Akhtar, and A. Ditta, "Secure framework enhancing AES algorithm in cloud computing," *Security and communication networks*, vol. 2020, no. 1, p. 8863345, 2020.

[28] V. Kakkad, M. Patel, and M. Shah, "Biometric authentication and image encryption for image security in cloud framework," *Multiscale and Multidisciplinary Modeling, Experiments and Design*, vol. 2, no. 4, pp. 233–248, 2019.

[29] M. Kaleem *et al.*, "New Efficient Cryptographic Techniques For Cloud Computing Security," *Migration Letters*, vol. 21, no. S11, pp. 13–28, 2024.

[30] P. Yong, Z. Wei, X. I. E. Feng, Z. Dai, G. Yang, and D. Chen, "Secure cloud storage based on cryptographic techniques," *The Journal of China Universities of Posts and Telecommunications*, vol. 19, pp. 182–189, 2012.

[31] S. I. Hamad, "Use of chaos in key schedules for a symmetrical encryption algorithm without data loss," *International Journal of Computational and Electronic Aspects in Engineering*, vol. 5, no. 4, pp. 194–202, 2024.

[32] J. M. Ragini Chavan, "Trust Model for Cloud Data Service Providers," *International Journal of Computational and Electronic Aspects in Engineering, RAME Publishers*, vol. 4, no. 3, pp. 86–89, 2023, doi: https://doi.org/10.26706/ijceae.4.3.20230905.

[33] Z. S. Karam, R. H. Ali, and B. O. Al-Nashy, "Exploring Emerging Strategies for Countering Computer Malware Attacks: A Comprehensive Survey of Tools and Techniques.," *International Journal of Computational & Electronic Aspects in Engineering (IJCEAE)*, vol. 4, no. 2, 2023.

[34] I. K. AI–Dulaimi, "The Use of Cloud Computing to Process Big Data: An Applied Study of the Virtual Library at the University of Mosul.," *International Journal of Computational & Electronic Aspects in Engineering (IJCEAE)*, vol. 4, no. 2, 2023.

[35] A.-A. A. Alsaiqal, "An Encrypting Electronic Payments Based on Kerberos Cryptography Protocol.," *International Journal of Computational & Electronic Aspects in Engineering (IJCEAE)*, vol. 5, no. 3, 2024.