Minimax Theory and its Applications
Volume 11 (2026), No. 2s, 700 to 712

Designing a Quantum-Resistant Secure Cloud Framework with Integrated Key Distribution and Multi-Party Computation

Devulapally Swetha[1], Jampani Satish Babu[2]

[1]Research Scholar Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur 522302, A.P., India, Email: swethanarayana32@gmail.com
[2]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur AP, India. Email : jampanisatishbabu@gmail.com

Abstract
With the rapid progress of quantum computing, traditional cryptographic methods have to face imminent hazards, especially in terms of the cloud environment, where data privacy and integrity are paramount. This research proposes a hybrid security structure that enables me to establish a quantum-flexible cloud architecture, Quantum Key Distribution (QKD), Post-Quantum Cryptography (PQC) algorithm, and Quantum Secure Multi-Party Computation (QSMC). The proposed model secures the cloud service layers service by embedding QKD for safe key exchange, quantum-resistant encryption, and pQC for authentication, and QSMC for Personalization PQC, and QSMC for Personalization. Software. QKD ensures tampering-proof key generation and delivery, while PQC mechanisms such as forged and based-based algorithms protect data and communication channels against quantum attacks. The simulation results display high major exchange success rates (up to 99.9%) and lower error rates with noise and long-distance content with admissible computational overheads. Display metrics, including encryption/decryption time, throughput, and quantum attack resistance, were strictly evaluated. The proposed solution proves effective for spontaneous integration in the existing cloud service model and provides a scalable path towards a quantum-mature cloud infrastructure. Finally, the framework establishes a safe, quantum-flexible communication environment, offering significant progress in cloud security against both classical and quantum threats.

Keywords: Quantum Key Distribution, Post-Quantum Cryptography, Kyber, AES-256, Cloud Security, Quantum-Resistant Encryption, Quantum Secure Multi-Party Computation

Introduction

Cloud computing has revolutionised the way data and applications have been stored, processed, and accessed by offering scalable, on-demand services on the Internet. It has become widespread in industries like finance, health services, education and government due to cost efficiency, flexibility and access[1]. Organisations are rapidly migrating to the cloud environment to take advantage of infrastructure as a service (IAAS), platforms as a service (PAA), and software in the form of a service (SAAS), reducing the need for physical infrastructure and IT maintenance[2]. However, as the data proceeds in the shared cloud infrastructure beyond the traditional organisational boundaries, new security and privacy challenges have come up. One of the most important concerns in cloud computing is protection, including data violations, unauthorised access, identity theft, refusal (DOS) attacks and many dangers, including insider danger[3]. Traditional cryptographic techniques like RSA, AES and ECC have been used to protect sensitive information through encryption, authentication and integrity investigation. While these methods are strong against classical computational attacks, they are not immune to the potential computational power of quantum computers[4].

Depending on quantum computing, the principles of quantum mechanics, a paradigm in computational capabilities, is introduced through features such as superposition, complication and quantum equality[5]. This emerging technique has the ability to solve problems considered infallible for classical computers, including the ability to break widely used cryptographic algorithms. For example, the noise algorithm can rapidly fail large prime numbers compared to the classical algorithm, threatening the RSA and the ECC[6]. Similarly, Grover's algorithm can accelerate the brute-force attacks on symmetric cryptography. Despite these dangers, quantum computing also offers important opportunities to increase safety, especially through QKD, QMSC and PQC. QKD allows the theoretically unwavering encryption to safely share cryptographic keys using the rules of quantum physics, while PQC focuses on developing new cryptographic algorithms that are resistant to quantum attacks[7]. The dual role of quantum computing – both as disruptive and ambitious – is mandatory to detect the

quantum-monotonised security mechanism for the future-proof cloud computing environment against the dangers that develop[8].

With the wide adoption of cloud computing in today's digital scenario, ensuring the safety of data and communication within the cloud has emerged as an important challenge. Traditional encryption methods - such as RSA, elliptical curve cryptography (ECC), and Advanced Encryption Standard (AES) - historically formed the core of the Cloud Security Protocol. These cryptographic algorithms depend on complex mathematical problems, such as integer factors and computational rigidity, to protect the privacy and integrity of sensitive data [9]. However, the emergence of quantum computing presents a significant danger to the preservation of these classical cryptographic schemes. Quantum computers can efficiently solve problems that are currently impossible for classical computers, with their ability to perform complex calculations at unprecedented speeds[10]. For example, the noise algorithm can cause a large integer factor in polynomial time, effectively compromising the safety of RSA and ECC. Grover's algorithm can accelerate brute-force attacks, reducing the effective security of symmetrical encryption methods. These abilities weaken the existing encryption protocol for quantum attacks, potentially highlighting the important data in the cloud environment to unauthorised access and tampering[11].

To address this looming danger, there is an immediate need to develop and integrate post-quantum cryptographic algorithms and quantum-prosperous security mechanisms in cloud computing architecture. Post-quantum cryptography aims to design algorithms that can withstand attacks from both classical and quantum computers, while quantum-prosperous methods such as quantum key distribution (QKD) take advantage of quantum mechanics to take advantage of quantum key distribution (QKD). Without active progress in these regions, cloud infrastructure becomes obsolete in the face of quantum-cinema hazards. Therefore, it is mandatory for future-proof cloud computing systems to be infection-proof towards quantum-flexible security structures. The primary objective of this research is to seriously analyse the existing security mechanisms employed in the cloud computing environment. It aims to detect quantum-based cryptographic solutions, including quantum key distribution and post-quantum cryptography. The study wants to design a quantum-prosperous security structure for cloud infrastructure. Finally, the proposed structure will be evaluated for its effectiveness, scalability and resistance to quantum hazards.

- Developed a hybrid cloud security framework combining Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) and Quantum Secure Multi-Party Computation to resist quantum attacks.
- Integrated quantum-safe mechanismsQuantum Secure Multi-Party Computation into all cloud service models (IaaS, PaaS, SaaS) for securing data at rest, in transit, and in use.
- Simulated and evaluated the performance of QKD and PQC using realistic cloud scenarios and standard quantum simulation tools.
- Demonstrated improved security metrics such as key exchange success rate, encryption/decryption time, and resistance to quantum attacks.

The remaining part of this study has been structured as follows: Section 2 seizure presents related functions on prediction, while Section 3 underlines boundaries in current methods. The details of Section 4 discussed the proposed deep learning-based approach, section 5 discusses the results and conclusions, and Section 6 concludes research.

Literature work

Liu et al.[12]state a post-quantum secure multi-party collaborative signature scheme with deterability for improved security and signature traceability in IIoT. The authors use lattice-based cryptography, specifically Learning With Errors (LWE), to be quantum attack-resistant and to provide multi-party signing. The scheme is beneficial in robust, traceability, and distributed industrial system scalability. Though the solution is problematic in terms of computational overhead and real-world deployment for IIoT devices with limited resources, although the results exhibit strong resistance against quantum-based attackers.

Qu and Wang [13]describe a secure multi-party quantum computation (SMQC) protocol on top of blind quantum computation by which clients outsource quantum calculations to a server without exposing inputs and algorithms to them. The technique integrates verifiable blind quantum computation and entanglement based on quantum into correctness and confidentiality. The scheme provides benefits such as strong privacy assurances and protection against server-side inference attacks. Nevertheless, the system is constrained by expensive communication overheads and the need for primitive quantum capabilities at the client side, although it remains secure under realistic quantum threat models.

El Azzaoui, Salim, and Park [14] suggest a quantum-assisted big data framework that combines quantum machine learning and quantum cryptography for effective and secure analytics. The approach employs quantum-enhanced algorithms to handle large datasets while maintaining data confidentiality using quantum key distribution. Its strength is enhanced processing speed, predictive accuracy, and secure data protection in IIoT networks. The complexity of the system's implementation and hardware constraints, however, are serious challenges, even if it is able to produce promising results in simulated environments.

Abidin et al. [15] discuss how quantum cryptography methods—particularly Quantum Key Distribution (QKD)—can be applied to advance secure communication and storage of data in MCC. They propose a solution that introduces mechanisms of authentication and encryption based on quantum for either replacing or reinforcing conventional cryptographic algorithms. Major benefits are resistance against brute-force and quantum attacks to provide long-term security for mobile networks. But constraints are the expense of quantum infrastructure and integrating it with existing mobile platforms, although the outcome indicates enhanced security resilience.

Padmanaban [16] suggest a hybrid model in which the AI algorithms take advantage of quantum speedup during training and inference when used in cloud-based systems. They leverage quantum annealing and quantum machine learning to process data-driven tasks such as optimization, pattern detection, and decision-making. The key benefit is the drastic decrease in computation time and enhanced efficiency in solving intricate issues. Challenges are limited quantum hardware availability, high error rates, and integration issues, although early implementations show better performance in some AI workloads.

Blanco, Santos-Olmo, and Sánchez [17] introduce QISS, which is a quantum-upgraded framework incorporating quantum key distribution and AI-based incident analysis for proactive and sustainable threat countermeasures. The approach utilizes quantum cryptography for confidential communication and applies machine learning to identify and categorize security incidents in real time. It provides benefits such as strong quantum attack resistance, energy efficiency, and adaptive response to threats. Challenges, on the other hand, are complex in the integration and scalability of quantum infrastructure in big IoT deployments, although the framework provides better detection accuracy and response time in test cases.

Problem Statement

With rapid adoption of cloud computing in various fields, ensuring safety and privacy of data stored in clouds has become a major challenge. Traditional cryptographic techniques such as RSA, ECC, and AES, although effective, are rapidly weakening in front of emerging quantum computing capabilities against classical threats[18]. Quantum algorithms such as Shor's and Grover's have been threatened with breaking widely used encryption methods, which is possible to compromise the integrity and privacy of potentially cloud-based systems. This creates a significant safety difference that can cause severe data violations and loss of confidence in cloud services. Therefore, there is an urgent need to detect advanced security mechanisms that are resistant to quantum attacks[19]. Quantum cryptographic algorithms and quantum-dominated technology promising solutions after offering quantum key distribution. Addressing this issue is important to create a flexible cloud security structure that is capable of understanding the future dangers generated by quantum computing progress.

Proposed Quantum secure cloud security

The proposed framework QKD, PQC, and Quantum secure multi-party calculation (QSMC) presents a comprehensive, quantum-flexible security architecture as a service (IAAS) as a service (IAAS) in all service layers as a service (IAAS) in all service layers. In the IAAS layer, QKD ensures unbreakable major exchange mechanisms between users and cloud infrastructure, taking advantage of the basic principles of quantum mechanics for safe communication. At the PAAS level, PQC algorithms such as forge-based and hash-based cryptography security application development, data transmission, and identity authentication against quantum hazards. At the mother -in -law, QSMC allows many sides to cooperatively calculate on encrypted data without revealing their personal inputs, thus ensuring privacy in shared services such as analytics and decision making. This integrated model provides a layered defense strategy that prevents current and future dangers-in which people are included by quantum computing-while enabling privacy conservation and safe cloud-based calculations for sensitive and mission-critical applications.

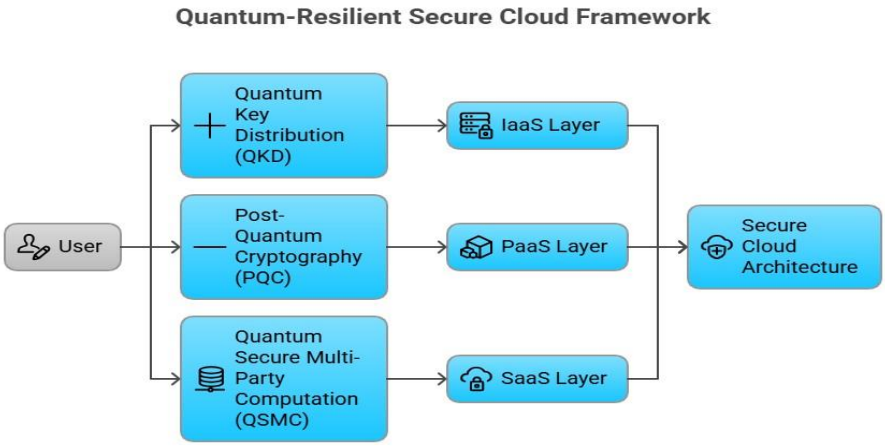


Fig 1 . Quantum Secure Cloud Framework

Development of a Hybrid Security Model for Cloud Environments

Quantum Key Distribution (QKD) fulfils the important task of enabling safe key exchange between cloud providers and users by taking advantage of quantum channels. In this process, cryptographic keys are transmitted using quantum states – usually photons – and the properties, such as polarisation, are replaced in such a way that any eavesdropping effort, quantum no-cloning theorem, measurement theorem, and measurement-and-comprehensive disturbances introduce detections. Protocols such as BB84 are used to install a shared secret key, where the sender encodes bits in quantum states and the receiver measures those using randomly chosen bases. After a public comparison of the base of the measurement, only the matching bits are maintained to create a raw key, which is later refined through error correction and privacy amplification. This ensures that the two sides share a safe, similar key, which cannot be intercepted or duplicated by any third party, even one equipped with quantum computing capabilities, which establishes a quantum-safe foundation for cloud communication. The following Fig.2 shows the working process of Quantum Key Distribution:

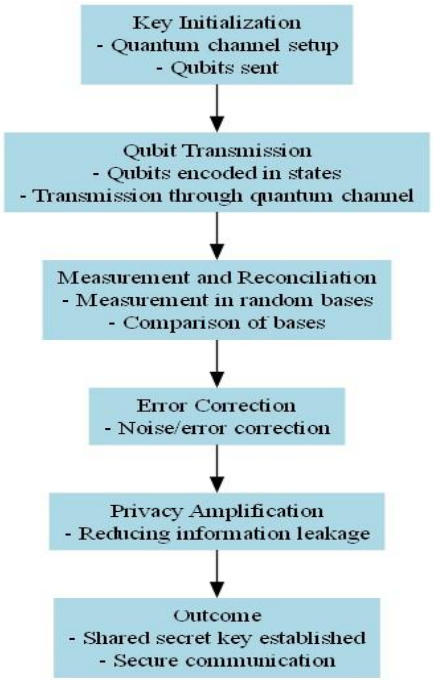


Fig 2 . Working Process of Quantum Key Distribution

Key Initialization

The first step in the QKD process is setting a quantum channel between the cloud provider and the user. This involves using the QKD protocol, such as BB84, to safely start the key exchange. The sender (cloud provider) and receiver (user) both agree to a specific method for encoding and decoding quantum bits (Qubits). The basic units of quantum information are sent to the quantum channel. This channel can be applied using various mediums, such as fibre optic cable or free space for satellite-based communication.

Qubit Transmission

Once the quantum channel is established, the sender encodes the qubits in specific quantum states. These states can represent polarisation, spin orientation, or other quantum properties of used particles. For example, in the BB84 protocol, qubits are encoded in one of the four potential states: two for vertical/horizontal polarisation and two for diagonal polarisation. Travelling through the quantum channel, the qubits are transmitted from sender to receiver. The main property of the quantum states is that they cannot be cloned or measured without any changes, ensuring that any evils will be able to find out the effort.

Measurement and Reconciliation

When obtaining the transmitted qualities, the receiver measures the quantum states using a randomly chosen base. This means that for each QIBIT, the receiver must decide whether it is measured at the same basis as the sender was used (for example, horizontal/vertical or diagonal). The sender and receiver then communicate on a classical but unsafe channel, which they use. They release any bits where the base is not aligned, as those bites will be incredible. The remaining bits, where both sides used the same base, are placed as part of the shared raw key. This procedure ensures that only the bits measured in compatible grounds are maintained, which creates the foundation of the secret key.

Error Correction and Privacy Amplification

Regardless of the safe nature of quantum key distribution, factors such as noise or potential eavesdropping can cause errors in the transmission process. The next step is the error correction, where the two sides work together to identify and correct errors in the raw key. This ensures that both sender and receiver have the same key. Privacy amplification is then applied to secure the key by removing any residual information, which can be leaked in an eavesdropper during transmission, especially if there were discrepancies at the error rate that indicate third-party participation. Privacy amplification reduces the amount of information that can be potentially exploited by an opponent, ensuring that the key is safe.

After error improvement and privacy amplification, the result is a shared secret key between the cloud provider and the user. This key is safe, even in the presence of quantum-capable opponents, as any attempt to intercept or measure the qubit during transmission would have disrupted the major exchange. The shared key can now be used for symmetric encryption, allowing safe communication between parties. This key security creates the foundation for security architecture, which allows the cloud provider and the user to encrypt and decrypt messages and data with a quantum-flexible encryption scheme.

Post-Quantum Cryptographic Algorithms

Post-quantum cryptography (PQC) includes a suite of cryptographic techniques designed to oppose attacks from quantum computers. Unlike traditional public-key cryptographic systems “(e.g., RSA and ECC)”, which are insecure for quantum algorithms such as noise and Grover, PQC plans are made on hard mathematical problems that are also infallible for quantum computers. These include lattice problems, hash functions, code-based cryptography and multivariate multiplication equations. In the proposed hybrid cloud security framework, PQC is used with QKD, which is to provide safe encryption, authentication and verification to provide safe key exchange for authentication and verification and a dual-level defence for PQC[20]. Figure 3 shows the hybrid cryptographic flowchart:

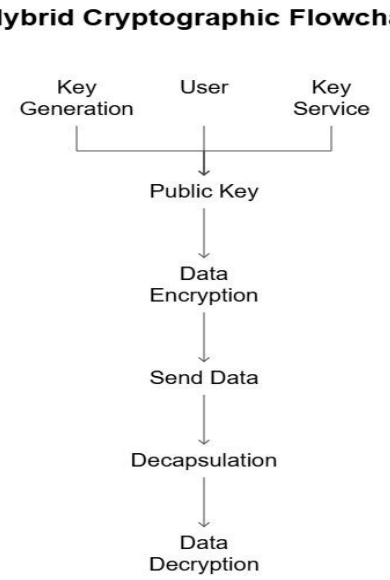


Fig 3 . Hybrid Cryptographic Flowchart

Key Generation Using Kyber

The major generation process in Kyber is an important initial step in installing a quantum-safe communication channel between a user and cloud server. Kyber is a lattice-based post-quantum cryptographic algorithm designed to oppose attacks from quantum computers. These errors (LWE) operate on the basis of learning with the problem, which is currently considered quantum-resistant. The process begins with the cloud server, which produces a pair of cryptographic keys: a public key and a private (secret) key. It is completed using the internal key generation algorithm of Kyber, which depends on the complex mathematical structures known as lattices.

The server first selects a security level, such as Kyber512, Kyber768, or Kyber1024. These cryptographic strengths and leading levels of major sizes are suitable; Kyber512 is suitable for mild applications, and Kyber1024 is used for highly safe environments. Once the level, Kyber gives a sample of a random polynomial from a predetermined distribution to generate noise and secret values. They are used to calculate a public matrix and a secret vector. By multiplying the polynomial matrix multiplication and noise, the algorithm ensures that the final key is impossible to compute or reverse-engineer – even for a quantum anti-engineer[21].

Key Encapsulation

In the second stage of the Kyber-based post-quantum cryptographic process, the user (client) begins safe communication by enacting a shared secret using a public key (PK) obtained from the cloud server. This step is known as the key encapsulation and is important to enable a safe session without sharing the symmetrical key directly. The user appoints the Kyber's enacting algorithm, which takes the public key of the cloud as an input and produces two outputs: a ciphertext (CT) and a shared secret (SS). The shared secret (SS) is essentially a randomly generated symmetrical key (for example, a 256-bit key) that the user will later use to encrypt its session data using a symmetrical encryption algorithm such as AES (Advanced Encryption Standard). Because the symmetric encryption is computably efficient, it allows safe and rapid data transfer after completion of the key exchange. Importantly, the user does not transmit this shared secret directly. Instead, they encounter it in a cipher text using the public key of the cloud and only send this cipher text (CT) to the cloud.

The encapsulation process works by combining the public key with the public key of the cloud using the first random values (usually in the form of a polynomial) and using lattice-based arithmetic. These operations produce a cipher text that hides the shared mystery within the composition of the lattice problem, ensuring that even though intercepted, the cipher text does not leak useful information about the key.

Algorithm: Key Encapsulation

Algorithm KeyEncapsulation(pk)

Input:
pk ← Public key from cloud server

Output:
ct ← Ciphertext sent to cloud server
ss ← Shared secret for encrypting session data

Steps:
1. Generate random seed r using a cryptographically secure random number generator
2. Derive ephemeral key (ek) and plaintext message (m) from r using a hash function
3. Compute ciphertext ct = Encrypt(m, pk) using Kyber encryption function
4. Derive shared secret ss = Hash(m || ct) using a secure hash function like SHA3-256
5. Return ct, ss

Hybrid Encryption Model: Kyber + AES-256

Kyber, a post-quantum key encounter mechanism (KEM), is employed to generate a shared secret between the user and the cloud server, which ensures strong security against quantum attacks. This shared mystery was once established through the quantum-resistant encryption process of Kyber, then used as a symmetrical key for AES-256 encryption. AES-256 is known for its high security and efficiency, encrypting the real user data, ensuring that even though the ciphertext is intercepted, the data remains inaccessible without the correct key. The framework cloud receives both quantum-flexible and performing-unfeated safe communication in the framework cloud environment, combining the key exchange for data encryption and the Kyber for AES-256.

Key Initialization using Kyber

The process begins with the cloud provider, which produces a key pair using the Kyber key generation algorithm, which outputs a public key (PK) and a private key (SK). This call (pk, sk) = kyber.keygen (). The public key (PK) is then shared on a public (but certified) channel with the user, while the private key (SK) is safely stored with the cloud provider. Kyber's forge-based construction-quantum ensures security, making it stronger against quantum computing hazards.

Shared Secret Generation (Key Encapsulation)

On receiving the public key PK, the user makes the key encapsulation using the Kyber Encapsulation function, the yield of a ciphertext CT, and a shared secret SS, which is calculated as (CT, SS) = Kyber. Encapsulate (PK). Ciphertext CT is a compressed, encrypted form of symmetrical key materials that can only be decapped by the holder of the respective private key SK. This is saved for transfer to CT cloud, while the user retains SS, which will be used to obtain a symmetric encryption key.

AES -256 Encryption and Decryption Process

The process in the hybrid encryption model that relies on Kyber and AES-256 guarantees quantum-resistant key exchange as well as productive symmetric encoding of data for safe transfer and saving. Once the shared secret (ss) is created by the user and the cloud provider working with Kyber's key encapsulation mechanism, it is not used for directly encrypting information. Instead, it is put through a processing using a Key Derivation Function (KDF) – like HKDF or any other SHA3 based functions – to derive a cryptographically secure and uniform 256 bit key for encryption via AES. This derived key known as AES _Key = KDF(ss) is essential in ensuring that the key material is of the right entropy and format for good encryption.

The Advanced Encryption Standard (AES), AES-256, is then used to encrypt the sensitive data of the user. AES-256 is a block cipher working on 128-bit blocks of data, which has 256-bit key for its transformation rounds, a highly secure cipher. The encryption is usually carried out in some secure mode of operation like Galois/Counter Mode (GCM) or CipherBlock Chaining (CBC). GCM is chosen where both the needs for data confidentiality and integrity are required, since it produces an authentication tag in addition to the ciphertext, but if the only requirement is confidentiality, CBC is used. The UserData can be transformed to EncryptedData= AES_Encrypt(UserData, AES_Key) using encrption process which makes it meaningless to unwanted parties.

After encryption, the encapsulated shared secret ss is then encapsulated by the Kyber ciphertext (ct) which is uploaded to the cloud together with the EncryptedData. Interestingly, ct does not disclose the secret but instead lets the cloud decap from it afterwards with the help of Kyber decapsulation function. When the cloud provider has to retrieve the data from the storage, it employs its private key (sk) and the stored ciphertext (ct) to reconstruct the shared secret in ss = Kyber.Decapsulate(ct, sk). This recovered ss is run through the same KDF giving the same 256-bit symmetric key (AES_Key) for encryption. Because each party generates this important key independently from the encapsulated shared secret, there is no need to actually pass on the key directly, so this presents a much lower intercept risk.

Finally, this derived key is used by the cloud provider to DecryptedData = AES_Decrypt(EncryptedData, AES_Key) decrypt the previously encrypted data to restore the original plaintext completely. This hybrid solution is able to integrate the post-quantum security of the Kyber lattice-based encryption, with the speed and reliability of AES-256, enabling scalable, solid cryptography for the protection of sensitive data on the cloud, particularly in a quantum world where the classic cryptographic methods may be compromised by these new machines of computation.

Quantum Secure Multi-Party Computation (QSMC)

Quantum Secure Multi-Party Computation (QSMC) is an advanced cryptographic technique designed to facilitate safe and privacy-conservative calculations between the opposing and many parties equipped with quantum computing capabilities. At its core, QsMC allows each party to contribute to other participants or external institutions to contribute private input data to a joint calculation process without disclosing the actual content of their input. It is particularly important in areas such as healthcare, finance, and government, where sensitive data (eg, patient records, financial transactions, or individual identifiers) cannot be exposed or centralized due to regulatory and privacy concerns. Unlike traditional multi-party computation (MPC), which depends on classical cryptographic beliefs that may be unsafe for quantum attacks, QSMC contains fake-based encryption and post-quantum zero-knowledge proofs such as quantum-resistant cryptographic primaries such as post-quantum zero-knowledge proofs. These encryphters ensure that even though a malicious actor has a quantum computer, they cannot break the confidentiality or integrity of the calculation. Through QSMC, institutions such as hospitals, banks, or research institutes can run cooperatively without compromising the privacy of a dataset on machine learning algorithms, statistical analysis, or decision-making processes, or rely on a trusted Central Authority.

Cloud Service Model Integration

The safe cloud architecture model has been designed to integrate state-of-the-art Quantum-Rigilant Technologies-QKD, PQC, and QSMC, which has three prominent layers of SaaS is infrastructure. Each layer addresses specific safety requirements and dangers, and hybrid integration of these quantum technologies also ensures end-to-end security in the presence of quantum computing hazards.

In the IAAS layer, which provides fundamental computing resources such as virtual machines, storage systems, and networking components, QKD is applied to install safe communication channels between cloud institutions and users. QKD takes advantage of mechanical principles - such as photon polarization - to generate and distribute cryptographic keys in such a way that any eavesdropping efforts change the quantum states, consume the system for potential intercourse. This makes the major exchange fundamentally safe, providing a tamper-tampering mechanism for distribution in session's key generation and physical and virtual infrastructure components.

In the PAAS layer, which offers development platforms and middleware services, PQC is included to secure the applications being developed and deployed. This includes the use of quantum-resistant algorithms such as fake-based, code-based, and hash-based cryptographic techniques, such as application-layer communications, authentication mechanisms, APIs, and data-in-transit protection. PQC ensures that even though a quantum attacker achieves access to encrypted materials or authentication data, they will be unable to break the cryptographic primitive within a viable time limit, thus preserving the integrity and privacy of the application services.

In the SaaS layer, which offers a full software application on the Internet, QsMC plays an important role in preserving privacy and enabling safe collaboration. QSMC allows many users or institutions to jointly calculate on their personal input (eg, healthcare data, financial records, etc.) without disclosing the actual data. It is obtained by distributing calculations in safe encrypted data shares and using a quantum-mature protocol that prevents information leakage. This ensures that services such as analytics, machine learning, or mother-in-law-

level services can process sensitive data without compromising user privacy-even against opponents equipped with quantum computational capabilities.

Collectively, it forms a quantum-flexible security structure for layered integration clouds, combining the physical-level protection of the QKD, the algorithm strengthening of the PQC, and the secrecy conservation of the QSMC. This architecture not only strengthens the defense mechanism in cloud stack, but also addresses the concerns of compliance and data sovereignty, making it ideal for important areas such as healthcare, finance, defense, and government services, which require the highest level of security assurance in the quantum era.

Result and Discussion

The simulation environment for evaluation of the proposed hybrid quantum-score framework was made using special equipment and a combination of virtual cloud architecture. Microsoft Quantum Development Kit (QDK) and IBM QISKIT were employed to follow the QKD protocol like BB84 and E91, which enables safe exchanges on quantum channels with variable noise and distance parameters. Post-Quantum Cryptography (PQC) algorithm, including Cabber and Sphinkus+, was integrated and tested using Cryptool and a Custom Python Implementation to simulate real-world encryption and authentication works. Framework was deployed in a layered cloud environment, which simulates IAAS, PAA, and SAAS models: QKD-secure key management and PQC-encrypted virtual machines were tested under IAAS; The safe session key and encrypted runtime data flow were managed under PAA; And SAAS applications were evaluated for safe user interactions and data integrity through PQC and QKD integration. This multi-level setup ensured a comprehensive evaluation of framework performance, scalability, and flexibility for quantum hazards in diverse cloud service models.

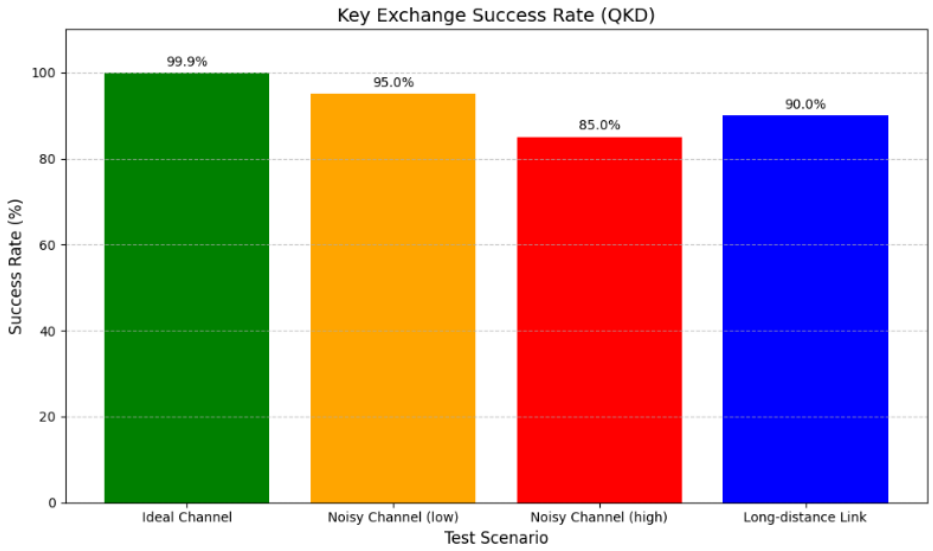


Fig 4 . Key Exchange Success Rate

Fig 4 summarizes the performance of a quantum key delivery (QKD) system under various test scenarios. Under ideal conditions without any external intervention, the system receives a close success rate of 99.9%. When exposed to low levels of noise, the success rate decreases by 95%, indicating minimal disruption in the major exchange process. However, in the high-end environment, the success rate decreases by 85%, suggesting that the intervention transmission greatly affects integrity. For long-distance links, such as QKD more than 100 km, the success rate is at 90%, indicating that the distance introduces some decline, the system maintains an appropriately high reliability in the extended boundaries.

Table 1. Key Generation & Encapsulation Time

Test Scenario	Key Generation Time (ms)	Key Encapsulation Time (ms)
Kyber512	150	300
Kyber768	200	400
Kyber1024	250	500
Ideal conditions	180	350

Table I Kyber512, the major generation time is 150 ms and takes the major encapsulation 300 ms, while Kyber768 requires 200 ms and 400 ms, respectively. Kyber1024, offering the highest security level, shows the highest time with 250 ms for the leading generation and 500 ms for encapsulation. In ideal conditions, the system is 180 ms for the leading generation and an average of 350 ms for encapsulation, reflecting the possibility of a balanced performance done without testing environmental or computational obstacles.

Table 2. Encryption and Decryption Times for Various Algorithms

Encryption Algorithm	Encryption Time (ms)	Decryption Time (ms)
AES-256 with Kyber512	50	40
AES-256 with Kyber768	70	60
AES-256 with Kyber1024	100	90
AES-256 (non-quantum)	30	25

Table II presents the encryption and decrypting time for AES-256 when the standard AES-256 is integrated with various key post-quantum algorithms compared to the encryption. AES-256 with Kyber512 records an encryption and decryption time of 50 ms and 40 ms, respectively, grows up to 70 ms and 60 ms with Kyber768, and up to 100 ms with Kyber1024 and up to 90 ms, adding computational loads for high security levels. Conversely, the standard AES-256 (non-quantum) is the fastest, with an encryption and decryption of 30 MS and 25 MS, respectively, over time, performs low delay, but lacks quantum-resistant features. Fig 5 and 6 shows the encryption and decryption:

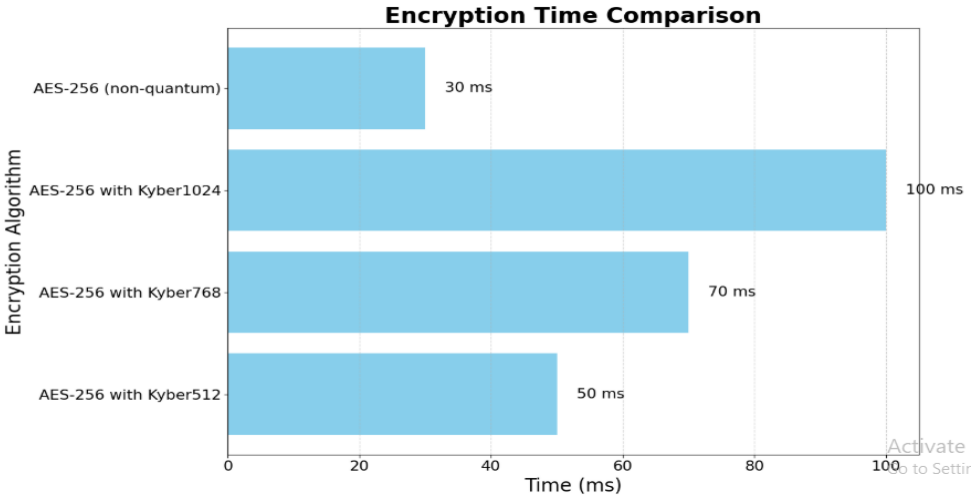


Fig 5 . Encryption Time Comparison

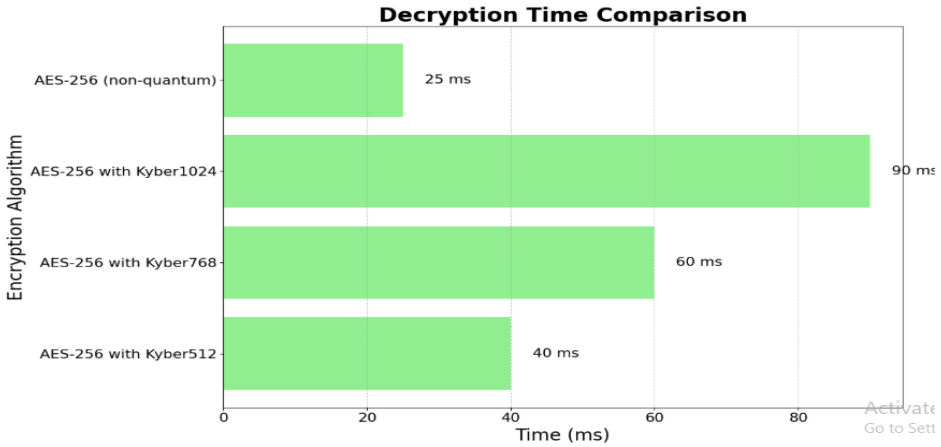


Fig 6 . Decryption Time Comparison

Fig 5 and 6metric measures the time taken to encrypt and decrypt the data using the PQC Encryption Scheme (eg, secret from the ciber of AES -256). Rapid encryption and decryption time reduces delay in real -time communication and data processing in cloud services.

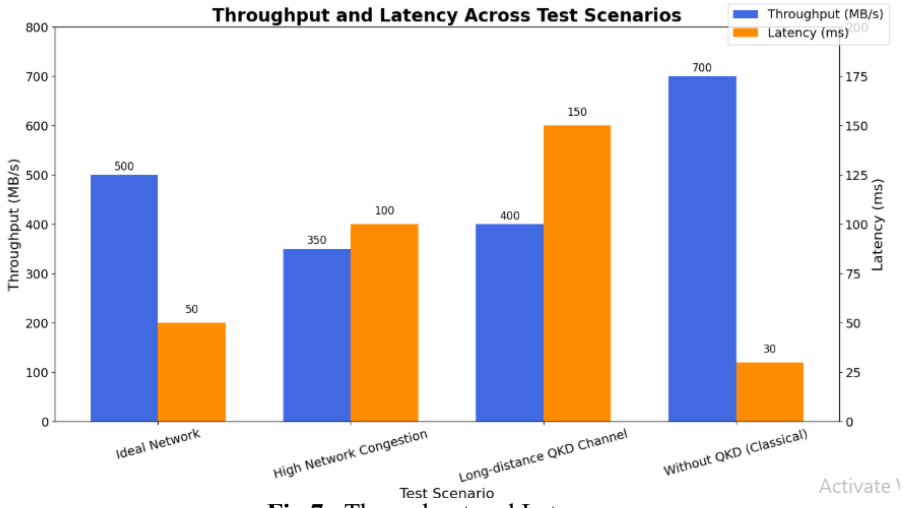


Fig 7 . Throughput and Latency

Fig 7 refers to the comparison of throughput and delay in four testing scenarios: ideal network, high network congestion, long-range CKD channels, and without QKD (classical). The landscape without QKD (classical) receives the highest throughput at 700MB/s with the lowest delay of 30ms, reflecting better performance but without quantum-level security. In contrast, long-range QKD channels reflect the low throughput of 400MB/s and the highest delay of 150 ms, highlighting the communication delay initiated by quantum key distribution at an extended distance. Under the ideal network conditions, the throughput is relatively higher at 500MB/s with a moderate delay of 50ms, while the high network congestion reduces performance up to 350MB/s and increases delays to 100ms. The graph displays trade-offs between network performance and security as introduced by quantum communication technologies.

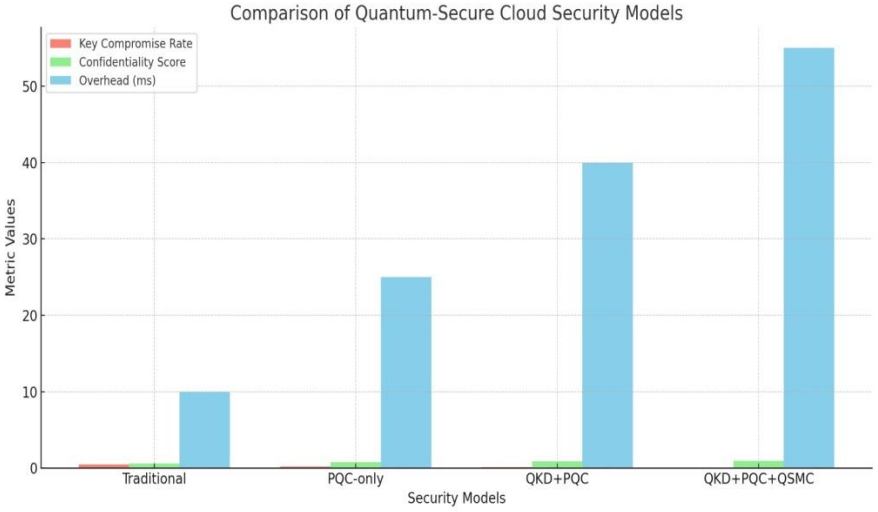


Fig 8 . Comparison of Quantum Secure Model

Fig 8 proposed QKD+PQC+QSMC safety model displays a significant decrease in the major agreement rate, multi-party

data processing achieves the highest privacy score of 0.95, and introduces medium computational overheads, which is appropriate due to increased privacy and security benefits

Discussion

This research presents a comprehensive investigation into a hybrid security structure in quantum-flexible cloud security, which integrates the QKD+PQC+QSMC in a hybrid security structure. Its purpose is to future-proof cloud infrastructure against the dangers generated by quantum computing-specifically noise and attacks capable by the algorithm of the Grover algorithm that can break the traditional encryption methods. QKD module takes advantage of the principles of quantum mechanics-especially the complication and no-cloning theorem, to securely generate and distribute cryptographic keys. The simulation result displays a high key exchange success rate (up to 99.9% in ideal conditions), with a tolerant decline under noise or long-distance conditions. The error rate remained within the acceptable margin, and quantum attack resistance was naturally strong due to quantum transmission and physical properties of measurement.

The PQC module uses quantum-resistant encryption technology, such as Kyber for Kyber for encapsulation and AES-256 data encryption. Across the separate security levels (Kyber512, Kyber768, Kyber1024), the system increased computational overhead but significantly improved the cryptographic strength. Encryption/decryption time remained within the practical range, even for high-protection caber variants, ensuring that the cloud service delay was minimal. Integration in three core cloud service models (IAAS, PAA, SAAS) was obtained through a modular design. For IAAS, virtual machines and data storage were preserved by QKD-secure key management and PQC encryption. In PAA, the runtime environment and API benefited from safe session handling and encrypted execution. The SAAS applications took advantage of safe communication and data security mechanisms without changing the user experience.

Overall, the results validate the viability of deploying a hybrid QKD+PQC+QSMC structure in a contemporary cloud environment. While QKD introduces logistic challenges such as hardware requirements and transmission noise, these are reduced through customized protocol selection (eg, BB84) and strong reconciliation methods. The PQC algorithm, although compared to classical cryptography, provides strong resistance against both classical and quantum attacks, making the trade-off worthwhile. Finally, this hybrid approach significantly increases the safety currency of cloud services, aligning them with the landscape of emerging quantum danger. It serves as a scalable and adaptable model to achieve data in distributed, multi-friendly, and delay-sensitive cloud systems-selects groundwork for future deployment in quantum-compatible infrastructure of the world.

Conclusion and Futurework

In the conclusion, the proposed hybrid security structure effectively enables making a flexible, privacy-conservation and quantum-preservation and quantum-preservation and quantum-preserving cloud computing architecture for the QKD, Post-PQC, and QSMC. By embedding these techniques in IAAS, PAA, and Saas layers, the framework ensures safe key exchange, strong data encryption, and confidential multi-sided calculation even in the presence of anti-quantum. This integrated approach not only strengthens cloud infrastructure against emerging quantum hazards but also increases data integrity, privacy, and user trust. Framework paves the way for future research and real-world implementation of quantum-safe cloud services, offering a permanent and scalable model for the next generation of safe computing environments.. In addition, it appoints quantum-resistant cryptographic algorithms such as Kyber, NTru, and XMS to ensure safe data encryption and authentication through PQC. All clouds are designed to operate in service models- IAAS, PaaS, and SAAS, ensuring data security for data-at-rest, in-transit, and in-use. Performance assessment shows high major exchange success rates (up to 99.9% in ideal conditions), acceptable encryption/decrying time, and strong resistance to quantum attacks. Integration viability and computational overhead are also evaluated, which confirms the practicality and adaptability of the framework. Future work will focus on implementing structure in a live cloud environment, discovery of integration with blockchain for data integrity, and improving the scalability of QKD for global deployment. Additionally, further tests against the real-world quantum-competent danger model will be conducted to strengthen the flexibility and readiness of the structure for the next generation cyber cybersecurity challenges.

References

1. D. Swetha and S. K. Mohiddin, “Quantum-Enhanced Security Advances for Cloud Computing Environments.,” International Journal of Advanced Computer Science & Applications, vol. 15, no. 6, 2024.

2. M. Emmanuel, “Quantum AI in Cloud Infrastructure: Preparing Enterprises for Quantum-Enhanced Machine Learning and Hybrid Computing Architectures”.

3. H. Padmanaban, “Quantum Computing and AI in the Cloud,” Journal of Computational Intelligence and Robotics, vol. 4, no. 1, pp. 14–32, 2024.

4. L. Tariq, A. Atta, U. Farooq, N. Anwar, M. Asim, and N. Tabassum, “Quantum-Inspired Cryptography Protocols for Enhancing Security in Cloud Computing Infrastructures,” Statistics, Computing And Interdisciplinary Research, vol. 6, no. 1, pp. 19–31, 2024.

5. U. Nauman, Y. Zhang, Z. Li, and T. Zhen, “Q-ECS: quantum-enhanced cloud security with attribute-based cryptography and quantum key distribution,” 2024.

6. K. Sondinti and L. Reddy, “Towards Quantum-Enhanced Cloud Platforms: Bridging Classical and Quantum Computing for Future Workloads,” Available at SSRN 5058975, 2023.

7. J. Jeffrey and D. Alexander, “Quantum AI for Proactive Threat Detection in Cloud-Edge Computing,” 2023.

8. M. I. Hossain, S. A. Sumon, H. M. Hasan, F. Akter, M. B. Badhon, and M. N. U. Islam, “Quantum-Edge Cloud Computing: A Future Paradigm for IoT Applications,” arXiv preprint arXiv:2405.04824, 2024.

9. E. U. Dibie, “Enhancing Cybersecurity for Renewable Energy with Quantum Algorithms and Cloud-Based AI,” Journal of Advances in Mathematics and Computer Science, vol. 39, no. 11, pp. 10–9734, 2024.

10. A. S. Rajawat, S. Goyal, C. Verma, and J. Singh, “Advancing network security paradigms integrating quantum computing models for enhanced protections,” in Applied Data Science and Smart Systems, CRC Press, 2025, pp. 517–528.

11. H. Alhakami, “Enhancing IoT security: Quantum-level resilience against threats,” Computers, Materials & Continua, vol. 78, no. 1, 2024.

12. J. Liu, J. Wen, B. Zhang, S. Dong, B. Tang, and Y. Yu, “A post quantum secure multi-party collaborative signature with deterability in the Industrial Internet of Things,” Future Generation Computer Systems, vol. 141, pp. 663–676, 2023.

13. G.-J. Qu and M.-M. Wang, “Secure multi-party quantum computation based on blind quantum computation,” International Journal of Theoretical Physics, vol. 60, no. 8, pp. 3003–3012, 2021.

14. A. El Azzaoui, M. M. Salim, and J. H. Park, “Secure and reliable big-data-based decision making using quantum approach in IIoT systems,” Sensors, vol. 23, no. 10, p. 4852, 2023.

15. S. Abidin, A. Swami, E. Ramirez-Asís, J. Alvarado-Tolentino, R. K. Maurya, and N. Hussain, “Quantum cryptography technique: A way to improve security challenges in mobile cloud computing (MCC),” Materials Today: Proceedings, vol. 51, pp. 508–514, 2022.

16. H. Padmanaban, “Quantum Computing and AI in the Cloud,” Journal of Computational Intelligence and Robotics, vol. 4, no. 1, pp. 14–32, 2024.

17. C. Blanco, A. Santos-Olmo, and L. E. Sánchez, “QISS: Quantum-enhanced sustainable security incident handling in the IoT,” Information, vol. 15, no. 4, p. 181, 2024.

18. N. Akhtar and A. Gilbert, “Quantum-Enhanced Cryptography: Safeguarding Blockchain and IoT Ecosystems,” 2025.

19. A. Barnabas and O. Matthew, “Exploring the Role of Quantum Computing in the Evolution of Edge and Cloud Solutions for IoT,” 2025.

20. S. A. Käppler and B. Schneider, “Post-quantum cryptography: An introductory overview and implementation challenges of quantum-resistant algorithms,” Proceedings of the Society, vol. 84, pp. 61–71, 2022.

21. F. Borges, P. R. Reis, and D. Pereira, “A comparison of security and its performance for key agreements in post-quantum cryptography,” IEEE Access, vol. 8, pp. 142413–142422, 2020.