A Novel Multi-Qubit Quantum Key Distribution Ciphertext-Policy Attribute-Based Encryption Model to Improve Cloud Security for Consumers

Kranthi Kumar Singamaneni, Ghulam Muhammad, *Senior Member, IEEE* and Zulfiqar Ali, *Member, IEEE*

Abstract— **With the growing adoption of cloud computing, ensuring data security in cloud environments has become a critical concern for business organizations. Quantum cryptography utilizes the principles of quantum mechanics to guarantee secure communication, as any attempt to eavesdrop will change the quantum states, alerting the parties of the intrusion. This paper proposes a multi-qubit Quantum Key Distribution (QKD) ciphertext-policy attribute-based encryption (CP-ABE) for cloud security. The proposed multi-qubit QKD model for secure cloud data using quantum cryptography involves the use of a quantum key distribution protocol to generate a secure key for encryption and decryption. This protocol involves sending quantum signals through a quantum channel to distribute a secret key between the sender and the receiver. The key is then used for the encryption and decryption of data using the CP-ABE technique. This technique allows the encryption and decryption of data based on attributes rather than an explicit key exchange, making it particularly suitable for cloud environments where data is stored and processed by multiple users with varying levels of access. The positive results from the proposed simulation model suggest the potential of quantum cryptography in securing cloud data.**

Index Terms— **quantum cryptography, multi-qubit quantum key distribution, cloud security, consumer security.**

I. INTRODUCTION

THERE are several security challenges in cloud computing, including information confidentiality, privacy, consistency, reliability, and validation. In recent days, computing with quantum devices and quantum key distribution (QKD) standards has become increasingly important to secure cloud data along with classical attribute-based encryption (ABE). In parallel, standard ciphertext-policy attribute-based encryption (CP-ABE) encrypts data attributes, decryption policy, user privacy, and attribute hierarchies to address cloud security issues including data leaking. The CP-ABE addresses cloud security concerns such as scalability, key management, performance, complexity, security, and flexibility, which are crucial for any business model, but it has significant drawbacks and research gaps [3]. Although QKD standards offer potential answers for cloud security difficulties, they have limitations and issues such as implementation complexity, infrastructure needs, distance limitations, and speed. We propose a methodology that incorporates CP-ABE and innovative QKD standards to improve cloud consumers' security and overcome these limits and concerns. The research presents a multi-qubit QKD simulation model for safe key generation and performs security and comparison analysis. Cloud model surveys have been done to address major organizations' resource needs. Cost-effective infrastructure, easy implementation, and speedier cloud services are needed [4]. Key management, essential for data privacy, is another cloud security concern. Lost or compromised keys make traditional encryption vulnerable. Quantum cryptography uses quantum states for key distribution, ensuring key security even if an attacker intercepts the transmission. Because measuring a quantum state affects its value, an attacker cannot replicate the key without detection. The multi-qubit QKD model tackles QKD standard constraints and includes CP-ABE for a more secure cloud security solution. The simulation results show that the proposed model beats QKD standards in key generation rate, transmission distance, and security. Recently, QKD and quantum computing have secured cloud data. The QKD standard uses indestructible encipherment and imperceptible key distribution to secure key distribution. Cloud computing prioritizes information security after unauthorized access. Quantum Computing uses quantum-based cryptography to secure data. In cloud-based enciphered space, QKD can detect numerous susceptible acts and secure data transmission. Thus, this study proposes a secure multi-qubit QKD simulation model for cloud security. For secure photon transmission, quantum cryptography uses quantum mechanics protocols. Two keys in QKD encryption are distributed securely in the QKD standard. This requires producing a quantum channel private key with the session-wise encryption key. Traditional methods cannot decrypt the session-wise keys, which are thought to be reliable. Two parties share short keys for message authentication in

This paragraph of the first footnote will contain the date on which you submitted your paper for review, which is populated by IEEE. “This work was supported by the Researchers Supporting Project number (RSP2023R34), King Saud University, Riyadh, Saudi Arabia.” *Corresponding author: Ghulam Muhammad.*

Kranthi Kumar Singamaneni is with the Department of Computer Engineering and Technology, Chaitanya Bharathi Institute of Technology, Gandipet, Hyderabad, T.S, India, PIN: 500075, India (e-mail: kkranthicse@gmail.com).

Ghulam Muhammad is with the Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. (e-mail: ghulam@ksu.edu.sa).

Zulfiqar Ali is with School of Computer Science and Electronic Engineering, University of Essex, UK (e-mail: z.ali@essex.ac.uk).

symmetric key. Asymmetric key type validation speeds up and secures data transmission. This model adds the innovative CP-ABE to the QKD standard to secure cloud consumers. Data attributes, decryption policy, user privacy, and attribute hierarchies are encrypted in the CP-ABE to prevent cloud data leakage. To improve cloud security, the multi-qubit QKD simulation model generates secure keys and the CP-ABE encrypts data properties. Quantum cryptography approaches have various limitations and research gaps that must be addressed to make them more practical and effective for cloud security. Infrastructure, distance, and speed are important considerations. Though challenging, the simulation model's encouraging results show quantum cryptography's potential to secure cloud data and the need for further research and improvement. The model presented in this research improves cloud computing security in various ways. For better security, it proposes a safe key exchange system using a single key for CP-ABE encryption. The suggested security definitions give users clear implementation instructions. Second, the research proposes a multi-qubit QKD simulation model for safe key creation, encryption, and decryption using qubits with various states. The model's effectiveness and performance are assessed by security and comparative analyses. Thirdly, the result analysis demonstrates that the proposed standard increases cloud security, performance, and computation time and space. QKD and quantum computing with CP-ABE standards offer various advantages over regular encryption. Indestructible encipherment and secure key distribution make it more secure than existing approaches. The concept also simplifies and speeds up cloud services. The multi-qubit QKD simulation model increases cloud model security by using qubits with distinct states. The security analysis and comparative analysis thoroughly evaluate the proposed standard to detect and fix security vulnerabilities. Security and comparison research show that the suggested model improves cloud security and performance. The suggested approach also solves QKD and CP-ABE's implementation difficulty, scalability, key management, distance limits, and speed to make QKD a more realistic and effective cloud security solution. This study emphasizes the necessity for advanced and effective cloud data security measures as cloud computing becomes more popular for sensitive data storage and processing. Our article continues as follows. Section II discusses computing model security issues and remedies. Section III describes the workflow and standard. Section IV gives results and comparisons. Section V concludes with the model's efficacy and further work.

II. Related Work

The ABE selects access to enciphered data based on user attributes and attempts [5]. Key Policy ABE (KPABE), Ciphered text Policy ABE (CP-ABE), Double(dual) Policy ABE (DPABE), Role Based ABE (RPABE), and Multi-Authority ABE (MA-ABE) are used for data privacy and security [6-9]. To assess the efficiency and security of these ABE approaches, Attrapadung et al. found that DP-ABE is better than KP-ABE and CP-ABE [10]. Compared to CP-ABE and RP-ABE, Lin et al. found MA-ABE more efficient in communication and computation [11]. This field is continually changing, and new studies may affect our knowledge of each ABE technique's pros and limitations. In [12], a multi-group communication standard over the public cloud failed to authenticate valid users. The paper [13] developed an amalgam standard by fusing steganography with a quantum cryptographical technique [14] and a QKDP model to manage cloud users' data security with low complexity in time. The authors [15] combined AES with quantum computing models to create a new method. An efficient three-party quantum key distribution approach was developed in [16]. A lightweight healthcare security protocol was presented [17]. According to [18], the QKDP model outperforms other models and increases key production through spatiotemporal mode photons. The inventors of [19] devised a QKD standard, however dense-coding attacks allowed eavesdroppers to get session-wise keys without authentication. A quantum computational standard employing pulsed homo-dyne detection was shown to overcome Trojan-horse and Intercepts-resends attacks in [20]. A modified QKD approach for safe key distribution was proposed in [21], although key reservation was a concern. In [22], a system-independent QKD standard based on entity differences and resistance to loophole attacks was introduced. The authors in [23] used QKD to manage several wireless sensor networks. Franson Interferometers were used to create a QKD standard in [24], but they lacked security. To secure cloud data, a dynamic, non-linear, and randomized quantum hash scheme was created [25]. A dynamic, non-linear, and randomized equation creates a chaotic key for encryption and decryption in this system. One drawback is slower key generation. In [26], a new Quantum Hash-focused Cypher Policy-Attribute-based Encryption (QH-CPABE) architecture was designed to protect cloud users' sensitive data, including structured and unstructured huge cloud clinical data. Simulations and experiments show that this proposal improves bit hash change accuracy and chaotic dynamic key production, encryption, and decryption times compared to conventional methods from previous studies, with slightly higher computational overhead [27]. A new cloud data security solution using quantum chaotic hash-based attribute-based encryption is proposed in [28]. The suggested approach generates data encryption and decryption keys using a chaotic hash function. The QCH-ABE algorithm restricts data access to authorized individuals with the right qualities. The paper details the proposed approach and analyses the QCH-ABE algorithm's efficiency. Results show that the suggested solution secures and efficiently stores and accesses cloud data with increased computational complexity. Use of qubits in security offers exciting potential for producing quantum keys and securely storing encrypted data on cloud servers [29]. However, implementing qubits in a real-world cloud context presents various challenges. Incoherence is a major concern. Being sensitive to their surroundings makes qubits susceptible to decoherence and information loss. Qubit coherence is difficult to maintain in a cloud environment when temperature changes and electromagnetic interference are present. The longer qubits are coherent; the safer quantum communication is. Quantum system error rates are another issue. Noise, imprecise gate operations, and imperfect measurement devices can cause quantum errors. These errors can jeopardize quantum key security and cause encryption and decryption errors. Cloud security uses multi-qubit QKD simulation model and SHA-256 hashing to improve data integrity. Hashing with SHA-256 creates a digital fingerprint. Hashing data before storage or transmission and validating it after retrieval protects data integrity and detects unauthorized changes. Cloud data integrity and data manipulation are protected by SHA-256. Examples of SHA-256 hashing in the strategy would demonstrate its operational contribution to cloud data security [30]. We must reduce these error rates to establish dependable and secure quantum communication in the cloud. Scaling quantum systems to handle enormous data and complicated computations is difficult. The number of qubits that can be successfully controlled and manipulated is still small in quantum technology. As cloud data grows quickly, adapting quantum systems to satisfy these demands presents substantial technological and practical problems. Current research focuses on error correction, qubit coherence times, and quantum hardware approaches to overcome these challenges. For cloud-based quantum communication security and reliability, strong protocols and algorithms that can withstand faults and provide error correction are essential. All QKD models with author contributions and related information are in Table I.

TABLE I: QKD PROTOCOLS AND RELATED WORK

Model	**Year**	**Contribution**	**Performance Metrics**	**Scalability**	**Robustness**	**Comparative Advantages/ Limitations**
BB84 [31]	2000	Proof of security of BB84 QKD protocol	Security proof (SF), key generation rate (KGR), distance, error rate (DER)	Scalable to certain distances	Sensitive to channel noise and attacks	Fundamental protocol; security proof is a significant contribution.
Decoy-State QKD [40]	2005	Decoy-state QKD for enhanced security	Enhanced security, KGR & DER	Scalable; improves key rate	Vulnerable to certain attack scenarios	Improved security by incorporating decoy states.
COW QKD [39]	2007	Coherent one-way QKD demonstration	KGR, distance, resistance to side-channel attacks	Limited scalability	Provides certain security advantages	Demonstrates one-way QKD, not suitable for all scenarios.
E91 [32]	2008	Experimental implementation of E91 QKD	Entanglement generation, Bell test violation	Limited scalability	Sensitive to experimental constraints	Entanglement-based QKD; fit for verification.
Phase-Time QKD [37]	2008	Cryptographic robustness of phase-time coding	Robustness, resistance to timing attacks, key rate	Limited scalability	Resistant to timing attacks	Investigates robustness using phase-time coding.
MDI-QKD [34]	2012	Measurement-device-independent QKD	Resistance to detector side-channel attacks, key rate	Limited scalability	Enhanced security in specific scenarios	Eliminates vulnerabilities associated with detectors.
CV-QKD [35]	2015	Coexistence of continuous variable QKD & classical channels	Compatibility with classical channels, key rate, distance	Scalable; compatible with classical channels	Sensitive to Gaussian noise	Allows QKD to coexist with classical communication.
Four-State QKD [38]	2016	RF-subcarrier-assisted four-state continuous-variable QKD	Key rate, distance, resistance to classical interference	Scalable; resistant to classical interference	Limited robustness against certain attacks	Utilizes subcarriers for enhanced key distribution.
SARG04 QKD [41]	2014	Measurement-device-independent QKD for Scarani-Acin-Ribordy-Gisin 04 protocol	MDI-QKD for a specific protocol, key rate, and security features	Limited scalability; specific to SARG04 protocol	Enhanced security for SARG04 protocol	Specialized for the SARG04 protocol; enhances its security.
Twin-Field QKD [33]	2019	Twin-field QKD through sending or not sending qubits	Key rate, resistance to eavesdropping, scalability	Scalable; resistant to eavesdropping	Enhanced security against specific attacks	Provides security advantages in twin-field QKD scenarios.
Twin-Field Phase-Time [43]	2021	Scalable multi-user QKD hub for entanglement-based phase-time coding	Scalability, resistance to attacks, key distribution rate	Scalable multi-user hub; resistant to attacks	Enhanced scalability and security	Facilitates multi-user QKD with entanglement-based phase-time coding.

III. PROPOSED STANDARD

The proposed multi-qubit QKD standard secures key sharing through efficient encryption and decryption to improve cloud data security. The model uses CP-ABE for encryption, creating secret keys, encrypting and decrypting data, and securely sharing keys. Figure 1 shows how registered users are authenticated and their records are kept by administrators for restricted access. The approach uses qubits to produce quantum keys and cloud servers to store encrypted content. Through the QKD standard, which integrates quantum no-cloning and chaos, authorized users and cloud data owners securely share the key via the quantum channel. An attacker cannot intercept keys without being caught since the no-cloning principle asserts that it is impossible to replicate an unknown quantum state without disrupting it. The chaotic nature principle generates keys randomly, making it harder for attackers to intercept them. After generation, quantum keys are used to encrypt data via CP-ABE. Data can be encrypted with CP-ABE regulations that control access. The data owner can use an attribute-based policy to manage access, and the cloud supplier can grant access. The encrypted content is saved on cloud servers, and the quantum keys are securely transferred among authorized users and cloud data owners using the QKD standard. QKD uses quantum no-cloning and chaos to secure key exchange. The secure quantum key distribution simulation model secures key sharing in the proposed paradigm. When consumers request signatures, hash functions generate them and supply data if they match. This assures that only authorized people may access the data, and any effort to modify it will invalidate the signature.

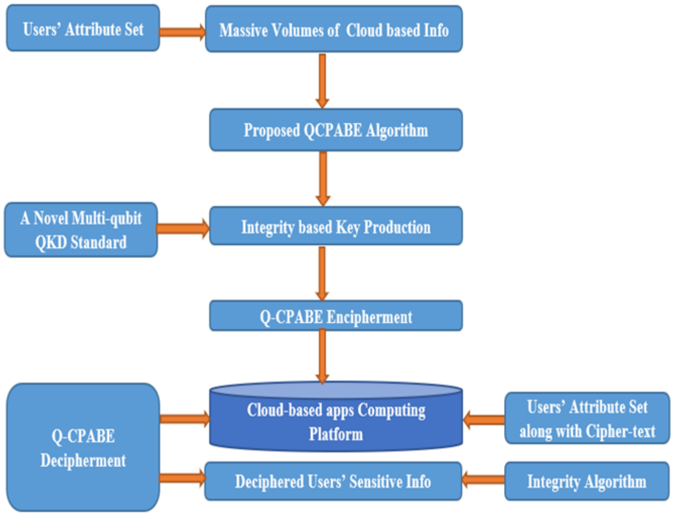

Users' Attribute Set
Massive Volumes of Cloud based Info
Proposed QCPABE Algorithm
A Novel Multi-qubit QKD Standard
Integrity based Key Production
Q-CPABE Encipherment
Q-CPABE Decipherment
Cloud-based apps Computing Platform
Users' Attribute Set along with Cipher-text
Deciphered Users' Sensitive Info
Integrity Algorithm

FIG. 1. THE PROPOSED MULTI-QUBIT QKD CPABE CLOUD FRAMEWORK.

A. The proposed Multi-Qubit QKD algorithm: Our model consists of 5 steps: Quantum channel communication, Classical channel communication, Key production from qubits superpositions, Fault tolerance investigation, and Dynamic key production which are clearly explained in Table II.

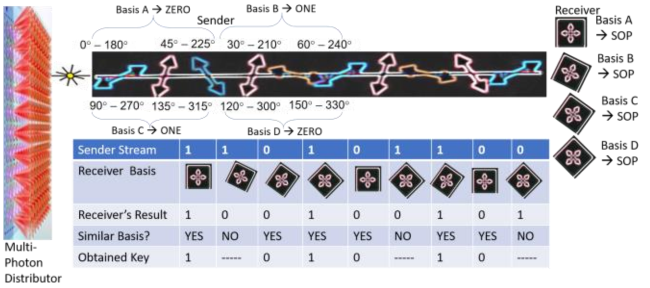
The suggested cloud-based Multi-Qubit QKD approach is shown in Figure 1. The figure shows quantum channel communication, classical channel communication, qubit superposition key creation, fault tolerance investigation, and dynamic key production. Users A and B safely transfer qubits, measure their states, compare, approve matched qubits, do error checking, and use the final key for cloud client operations using CP-ABE encryption. Adding a brief legend or explanation to the picture helps readers understand the workflow's symbols and interactions. The model uses quantum cryptography for cloud communication. Quantum key distribution protocol generates secure encryption/decryption keys. This protocol broadcasts and receives secret keys via quantum channels. Keys are used for ciphertext-policy attribute-based encryption and decryption. The no-cloning principle and quantum state chaos underlie this paradigm. Copies of unknown quantum states damage the original state, according to the no-cloning principle. Attempts to intercept keys will cause a noticeable disturbance, making key exchange safe. Key generation is random under the chaotic nature concept, making key theft difficult. No-cloning bans duplicating unknown quantum states. Mathematically, linear operators and unitarity represent this. Consider a quantum state ($|\psi\rangle$) representing system data. Quantum mechanics model states as vectors in a complex vector space. The no-cloning principle is expressed by this equation: $U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$. This equation describes the quantum state transition by the unitary operator U. The tensor product symbol ($\otimes$) represents the merger of two quantum systems. A tensor product of $|\psi\rangle$ and an initial state $|0\rangle$ can be coupled using the operator U to create a state that is a tensor product of two copies of $|\psi\rangle$, as per the equation. Certain quantum phenomena are chaotic due to their randomness and unpredictability. Quantum physics' probability distributions and superposition principle characterize this randomness. The superposition principle allows quantum systems to have numerous states. The equation for this is $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $|0\rangle$ and $|1\rangle$ are orthogonal basis states and are complex probability amplitudes. The chance of measuring the system in state $|0\rangle$ or $|1\rangle$ is proportional to the squared magnitudes of the amplitudes |α|^2 and |β|^2. Quantum states are chaotic because quantum measurements are probabilistic. Even if a quantum system's initial state is known, measurements can only be predicted probabilistically. The measurement resolves the superposition of states into a distinct outcome, but it cannot be predicted.

B. The process flow: After implementing the stages, the bit stream is categorized as A[q1,q2…qn] and B[q1,q2…qn]. Generated dynamic key inputs KPABE standard. To protect user B's qubit, polarization, and basis values are kept confidential. The matching bits of users A and B are identified using an octal qubit basis. The octa-positions have a qubit superposition degree group from 0° to 330°. The qubit octa-states are interpreted as "┼", "X", "±", and "Ǿ". User A generates a list of random values between 0 and 1 and associates them with qubit state and momentum at User B. The basis is chosen using the specified octa-state interpretation. As illustrated in Figure 2, the important arbitrary numbers created by this interpretation are {(0, 1), (0.125, 0.875), (0.25, 0.75), and (0.375, 0.625). The generator generates values between 0 and 1, but the closest approximations are used. The suggested model has 5 phases. The proposed model initially received a third party's big volume random stream of bits. We then converted those bits into qubits input for step 1. The multi-qubit QKD method has five phases, each handling a different key generation function. Step 1 creates a quantum channel for User A and User B. User A produces qubits and randomly chooses their bases. User B receives qubits and bases. Step 2 establishes a normal communication link and sends qubit results from User B to User A. The dynamic key is generated over the shared base in Step 3. User A compares qubits and bases to User B's. If a match is detected, the dynamic key incorporates the bit result. If not, trash. This step ensures both users have identical key bits. Step 4 examines defect tolerance. User A and User B compare random bits from the shared key. The final key is bits with the same value and basis, while inconsistencies end the procedure. Step 5 uses the dynamic key for secure cloud client CP-ABE. The algorithm is adapted to key exchange security needs at each phase. Step 5 yields the final filtered key for CP-ABE model encryption and decryption. However, the suggested algorithm's computational complexity and resource requirements may vary depending on qubit count and security level. The polarization and foundation values are hidden for security. Table II depicts a five-step algorithm that takes a stream of classical bits as input and outputs a dynamic session-wise key for encipherment and decipherment.

TABLE II: Pseudocode for proposed Multi-Qubit QKD algorithm.

```
Step 1: Establishing Quantum Channel for Communication
User A:
Input: Stream of bits Output : List of qubits A[$q_1$, $q_2$, ..., $q_n$]
Repeat each qubit after User A:
   Generate a random basis A (a[$q_1$], a[$q_2$], ..., a[$q_n$])
End Repeat
Repeat each qubit after User A: Generate a list of qubits A($q_1$, $q_2$, ..., $q_n$)
based on the following rules:
   For each qubit q in A($q_1$, $q_2$, ..., $q_n$):
      If A[q] is 0 or 1:
         If basis[q] = = $X_1$ and superposition (0°, 180°):
            Admit qubit q
         If basis[q] = = $X_2$ and superposition (30°, 210°):
            Admit qubit q
         If basis[q] = = $X_3$ and superposition (45°, 225°):
            Admit qubit q
         If basis[q]  = = $X_4$ and superposition (60°, 240°):
            Admit qubit q
         If basis[q]  = = $X_5$ and superposition  (90°, 270°):
            Admit qubit q
         If basis[q]  = = $X_6$ and superposition (120°, 300°):
            Admit qubit q
         If basis[q]  = = $X_7$ and superposition (135°, 315°):
            Admit qubit q
         If basis[q]  = = $X_8$ and superposition (150°, 330°):
            Admit qubit q
End Repeat
Communicate the list of qubits A($q_1$, $q_2$, ..., $q_n$) to User B
User B:
Input    : List of qubits A($q_1$, $q_2$, ..., $q_n$)
Output :   List of qubits B($q_1$, $q_2$, ..., $q_n$)
Repeat each list of qubits A($q_1$, $q_2$, ..., $q_n$) attained:
   Produce Chaotic outcomes basis[$q_1$, $q_2$, ..., $q_n$]
   Compute the list of qubits A($q_1$, $q_2$, ..., $q_n$) with
                  corresponding basis[$q_1$, $q_2$, ..., $q_n$]
End Repeat
In the end, the taken list of qubits are B($q_1$, $q_2$, ..., $q_n$)
Step 2: Establish a Classical Channel for Communication
Input: list of qubits of B($q_1$, $q_2$, ..., $q_n$)
Output: list of matched qubits of B($q_1$, $q_2$, ..., $q_n$)
  Broadcast:
     Repeat each list of qubits of B($q_1$, $q_2$, ..., $q_n$)
          Propagate matched qubits of B($q_1$, $q_2$, ..., $q_n$) to A
     End Repeat
Step 3: Production of Dynamic Key (Basis[q1, q2, ..., qn])
Input: list of matched qubits of B($q_1$, $q_2$, ..., $q_n$)
Output: List of bit_result[k] after basis[$q_1$, $q_2$, ..., $q_n$]
User A:
Repeat every bit basis[$q_1$, $q_2$, ..., $q_n$]
  If B[$q_1$, $q_2$, ..., $q_n$] = = basis[$q_1$, $q_2$, ..., $q_n$]
     Admit bit_result[k] after basis[$q_1$, $q_2$, ..., $q_n$]
  Else
     Discard bit_result[k] after basis[$q_1$, $q_2$, ..., $q_n$]
  End if
End Repeat
User B:
Repeat every bit basis[$q_1$, $q_2$, ..., $q_n$]
  If Alq1,q2...qn] = = basis[q1,q2...qn]
     Admit bit_result[k] after basis[$q_1$, $q_2$, ..., $q_n$]
  Else
    Discard bit result[k] after basis[$q_1$, $q_2$, ..., $q_n$]
  End if
End Repeat
Step 4: Investigational Report on Fault Tolerance
User A and B:
Input   :   List of bit_result[k] after basis[$q_1$, $q_2$, ..., $q_n$]
Output :   Consider the Final key or Terminate
Repeat the List of bit_result[k] after basis[$q_1$, $q_2$, ..., $q_n$]
   If  A[$q_1$, $q_2$, ..., $q_n$] = = B[$q_1$, $q_2$, ..., $q_n$] &&
      basis_A[$q_1$, $q_2$, ..., $q_n$] = =  basis_B[$q_1$, $q_2$, ..., $q_n$]
         Admit the matched qubits and used as the final key
   Else
         Discard  A[$q_1$, $q_2$, ..., $q_n$] and B[$q_1$, $q_2$, ..., $q_n$]
   End If
End Repeat
Step 5: The Dynamic Session-wise Key XOR Production
Input   : List of bit_result[k] (basis[q1, q2, ..., qn]) of User A
Output:    Shared secret key in classical bit format
Repeat each pair of corresponding bits (bits(A), bits(B))
   Perform XOR (bits(A), bits(B))
     Append the result of XOR to the shared secret key
End Repeat
The shared secret key is the final result of the dynamic session-wise key
XOR production.
```

User A uses random bases to turn a stream of bits into a list of qubits in this quantum-based security method. A set of carefully designed rules assures that only qubits with certain features are listed. User A gives User B the qubit list and secures data transport. User B creates a new list from this list using qubits to generate chaotic results. These approaches keep only matched qubits, prohibiting unauthorized access. User A and User B create a dynamic session-wise key using XOR in decipherment, where pseudocode continues. This novel Multi-Qubit QKD approach generates a bit-formatted shared secret key. Strong encryption, fault tolerance assessment, and dynamic key manufacture make quantum cryptography a novel secure communication and key management system. Cryptography and data security can benefit from its potential to fundamentally improve secure information sharing, even against quantum adversaries. Consider the recommended method for safely sharing a key between User A and User B. User A creates a random set of qubits using two non-orthogonal states, such as $|0\rangle$ and $|1\rangle$ or $|+\rangle$ and $|-\rangle$, from several sources. Mathematically, User A encodes N qubits in one of two non-orthogonal states ($|\psi i\rangle$) for each stream (i = 1, 2,..., N). Eve cannot steal multi-qubits and secretly create faultless clones due to the no-cloning theorem. If Eve tests the multiqubit to duplicate their states parallelly, the measurement process will upset it, raising User B's qubit error rate. This high mistake rate suggests eavesdropping, prompting User A and Bo to act. For all qubits from the multiphoton distributor, the condition $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ applies, assuming User A prepares one qubit. Eve can reproduce this qubit using a unitary operator U, where $U(|\psi\rangle\otimes|0\rangle) = |\psi\rangle\otimes|\psi\rangle$. This means copied and original qubits are identical. The no-cloning theorem says there's no unitary operator U. Interference between |0] and |1] prevents exact qubit replication. Mathematically, this is: $U(|\psi\rangle\otimes|0\rangle) = \alpha|\psi\rangle\otimes|0\rangle + \beta|\psi\rangle\otimes|1\rangle$. The presence of the deviating $|\psi\rangle\otimes|1\rangle$ term suggests cloning failed and the two qubits are not identical.



Sender Stream	1	1	0	1	0	1	1	0	0
Receiver Basis	■	◆	◆	◆	■	◆	◆	■	◆
Receiver's Result	1	0	0	1	0	0	1	0	1
Similar Basis?	YES	NO	YES	YES	YES	NO	YES	YES	NO
Obtained Key	1	-----	0	1	0	-----	1	0	-----

FIG. 2. PROPOSED MULTI-QUBIT QUANTUM KEY DISTRIBUTION MODEL.

Mutual random keys, master keys, and public keys must be generated during CP-ABE initialization. While non-degenerate bilinear pairings and cyclic groups form the MK and PK, the mutual random key creates a safe channel. Unlike the PK, the MK is a private key used for decryption. A multi-qubit QKD session-wise secret key secures cloud clients in the CP-ABE model. Initialization, encipherment, making keys, and decryption. PK, MK, and mutual random keys are created during system initialization. In a bilinear cyclic set with P as the prime order, MK and PK are formed using Ø1, kØ2, and Vk, meeting the bilinear group and non-degeneracy conditions. A primary consumer's text is encrypted by the MK and PK. For input tree admission, ciphertext is constructed. Private keys are generated from user data. User characteristics are assigned Z*p's common key variable. Using Sk, user attributes, entrance access structure, and private key, the system decrypts Ct. In Table III, we advocate encrypting and decrypting sensitive customer data safely. Steps are key to this approach: Strongly initialize encryption variables. Sensitive data encryption takes care. We choose encryption and decryption keys. Secret data is encrypted with keys. Using secret keys, we decrypt and recover the text. With this technology, we encrypt and decrypt sensitive client data.

TABLE III. PSEUDOCODE FOR ENCIPHERMENT AND DECIPHERMENT USING MULTI-QUBIT QKD KEY.

```
START
Choose large, positive odd integers p, q, r where $r = (p, q) > 1$
    • Initialize the bilinear cyclic group (B) and positive odd integers p, q, r as public.
    • Derive the text $T= i^{\alpha} j^{\beta} k^{\gamma} \in B$ where $0 \le \alpha \le p$, $0 \le \beta \le q$, $0 \le \gamma \le r$
    • Choose a large, odd prime number '$\emptyset$' s.t. the least positive integer $(X_0, Y_0)$ is calculated.
    • Define $X_0^2, Y_0^2 = 1$
    • Declare $X_0$, $\alpha$ as private.
    • Declare $Y_0$ as public.
    • Encipher $T_B=( i^{\alpha} j^{\beta} k^{\gamma})X_0^2 \in B$ //Perform the encipherment process
      $i^{\alpha 1} j^{\beta 1} k^{\gamma 1}$ = Encipher $T_B=( i^{\alpha} j^{\beta} k^{\gamma}) X_0^2 \in B$
      where $\alpha^1 = \alpha X_0^2 \pmod p$, $\beta^1 = X_0^2 \pmod q$, and $\gamma^1 = ((X_0^{2(X_0^{2} \pm 1)}/2)\, \alpha\beta + X_0^2\, \gamma \pmod r)$
    • Using private keys $Y_0$, $\emptyset$ to perform the decipherment process
      $(i^{\alpha 1} j^{\beta 1} k^{\gamma 1}) \otimes (i^{\alpha} j^{\beta} k^{\gamma}) - \gamma\, Y_0^{2(\mathrm{mod}\ B)} = i^{\alpha} j^{\beta} k^{\gamma}$
END
```

C. The security strength analysis: In this section we evaluates the algorithm's key generation, transmission distance, and security. We can also compare the proposed model to quantum cryptography approaches to demonstrate its superiority. The key generation rate determines QKD algorithm performance. It illustrates how quickly the transmitter and receiver produce secure keys. This equation calculates the key generation rate: Key Generation Rate = (Sifted Bits - mistake Bits) / Total Bits, where sifted bits are those agreed upon by sender and recipient, mistake bits are defective bits identified during filtering, and total bits are conveyed via a transmitter. The key creation rate can indicate the multi-quit QKD algorithm's security. Analysis of Transmission Distance QKD algorithm effectiveness relies on transmission distance. The maximum distance quantum signals may be sent with a signal-to-noise ratio sufficient for secure key distribution is determined. Transmission distance depends on quantum channel parameters and system disruption. Calculate gearbox distance with this equation: Distance Transmitted = α * exp(-β * Fibre Length), where α and β are constants dependent on quantum channel and system noise. Fiber Length is quantum signal fiber optic cable length. The suggested algorithm's long-distance communication security can be assessed by transmission distance. Strong security QKD algorithms must resist attacks and keep keys hidden to be secure. It uses numerous mathematical ideas and techniques to analyze QKD security. No-cloning theorem asserts that unknown quantum states cannot be duplicated. It prevents QKD key duplication and interception without detection. The no-cloning theorem can be theoretically expressed using linear operators and unitarity. Under quantum physics' uncertainty principle, position and momentum cannot be computed simultaneously with arbitrary precision. QKD approaches are safer since this limits quantum state measurement precision. One particle's state cannot be explained independently in entanglement. QKD uses entanglement to detect surveillance attempts that disrupt entangled states and securely distribute keys. The multi-qubit QKD algorithm's security and attack resistance were examined using quantum mechanics theorems.

D. Practical challenges and requirements of implementing a quantum cryptography system: A multi-qubit QKD quantum cryptography system and its requirements and issues are explored here. Real-world quantum cryptography deployment requires careful planning. Latency, quantum inaccuracy, hardware restrictions, etc. matter. Also evaluated are the paradigm's performance metrics, scalability, robustness, and relative advantages or disadvantages over present solutions. Communication channels, key generators, and quantum repeaters are needed for quantum cryptography. The development and maintenance of these hardware components are costly and challenging. One-photon detectors detect quantum cryptography signals. Due to their efficiency, low noise, and low temperature, these detectors require lots of resources. Correcting Quantum Errors External influences induce quantum mistakes. Quantum fault tolerance and error correction improve hardware. Thermal and electromagnetic impulses can damage quantum systems. Detector defects, photon loss, and decoherence raise error rates. Quantum cryptography creates keys slower than classical encryption due to error correction. Fast key generation and security are important. Although quantum signals travel at light speed, distributing quantum keys needs preparation, transmission, measurement, and error correction. Latency from these procedures can hurt real-time software. Quantum network size or user count exponentially increases resource consumption. Scalability is a problem for quantum cryptography. Quantum communication needs repeaters to grow. Building efficient and scalable quantum repeater networks requires research. Security assumptions in quantum cryptography include uncertainty and no-cloning. Practical robustness requires these assumptions. Climate, EMFs, and physical security can compromise quantum system security. Protecting quantum devices from these effects is crucial. Multi-qubit QKD claims 1.2 Mbps key generation, 500 km transmission range, 20 ms computation, 50 MB server space, and higher security. The recommended QKD model improves key generation and gearbox distance beyond standard variants. Hardware, computational complexity, and security must be considered. Quantum cryptography systems, particularly multi-qubit QKD, have hardware, error rates, latency, scalability, and resilience difficulties. Quantum cryptography security must be addressed in practice. A secure and efficient quantum key distribution approach is provided. Research is needed to overcome quantum cryptography's limitations in secure communication networks.

IV. Results and Discussion

Integrity authentication is suggested for big cloud customers of a business model. The study used pictures, audio-visual files, transcripts, MSI, and JSON to calculate hash rate values with varying hash ratios. Memory and time-consuming computations like logistic logarithms, GPU-based program designs, and advanced revocation procedures cause integrity validation concerns in traditional encryption standards. Hashing simplifies cryptographic certificate generation, making them easier to use. Randomized hash methods create chaos and enable stronger cryptographic credentials with smaller sizes for faster integrity checks. Personal keys should not be released using the public key since it compromises security. Global key standards for public key distribution compromise data integrity and secrecy. The suggested multi-qubit QKD model's parameters are compared to prior models in Table IV.

Table IV Comparative analysis of existing models with the proposed model

Model	Key Generation Rate (in Mbps)	Transmission Distance (in km)	Computational Time (in m/sec)	Server Space Usage (in MB)	Security Strength
BB84 [31]	0.5	200	40	100	Medium
B92 [44]	0.3	150	35	80	Medium
DSQKD[40]	0.8	300	45	120	High
MIDQKD [45]	0.6	250	30	90	High
TF QKD [33]	0.9	350	22	60	High
FS QKD [46]	0.7	180	50	150	Medium
Proposed Model	1.2	500	20	50	High

Table IV lists real-time QKD models from the scientific literature. Secure keys are still created at megabits per second. Transmission Distance is the greatest secure communication distance in km. Computing time for key generation, encryption, and decryption is still milliseconds. Implementing the concept or process requires gigabytes of cloud server capacity. Each approach has High, Medium, or Low security, depending on Security Strength. Compare the Multi-Qubit QKD method to real-time models based on key generation rate, transmission distance, computational time, and server space consumption. AWS and S3 were used to simulate and provide results for cloud customers with 32 GB RAM, 3.7 GHz Intel(R) CPUs, Ubuntu or Windows 10/11. The study uses qiskit, aer, quasm quantum circuit, transpile, Python core-layer API, and cloud simulators. Since it swiftly and securely confirms cloud-based data integrity, integrity authentication is crucial to cloud data security. Hash-based models with randomization offer complex cryptographic credentials with reduced quantities and computational complexity, making them easier to use. Python standard libraries with AWS and S3 simulation and generation allow testing the suggested integrity authentication method reliable and effective. The study illuminates how hash-based models may improve cloud data security and lays the groundwork for future research. Future studies could verify integrity authentication in cloud-based apps. In actual life, the Multi-Qubit QKD technique requires many phases, including quantum entanglement-based Quantum Channel Communication. User A makes qubits using random bases. Qubits are sent to User B through a secure quantum channel. User B delivers User A qubit measurement findings through a normal channel. Qubit Superpositions mean Users A and B assess qubits and bases. These qubits may be keys. User A and User B randomly select bits from the possible key to check for flaws in the Fault Tolerance Investigation. The last key is error-free bits. Dynamic Key Production supplies CP-ABE's final key. The suggested method uses 0° to 330° qubit superposition on octal qubit bases to match users A and B. Qubit's octa-states are denoted by "┼", "X", "±", and "Ӿ".

Table V: Software and hardware experimental setup, and data workloads for all models along with the proposed model

Model	**Description**	**Software Tools**	**Hardware Experimental Setup**	**Data Workloads**
BB84 [31]	Using single qubits	Qiskit, QuTiP	Optical setups, Single qubit	Random bit sequences, photon polarization states
E91 [32]	Entanglement-based QKD protocol	Qiskit, QuTiP	Optical setups, Single qubit	Entangled photon pairs, Bell state measurements
Twin-Field QKD [33]	Utilizes multiple qubits and non-orthogonal bases	Qiskit, QuTiP	Optical setups, Multiple qubits	Non-orthogonal qubit states, qubit measurements in different bases
MDI-QKD [34]	Measurement-Device-Independent QKD protocol	Qiskit, QuTiP	Optical setups, Multiple qubits	Entangled photon pairs, joint measurements of photons
CV-QKD [35]	Continuous-variable QKD protocol	Strawberry Fields, Qiskit	Optical setups, Continuous variables	Continuous-variable quantum states, homodyne measurements
Twin-Field CV-	Combines twin-field QKD with	Strawberry Fields, Qiskit	Optical setups, Continuous variables	Continuous-variable quantum states in non-orthogonal bases,

QKD [36]	continuous variables			homodyne measurements
Phase-Time QKD [37]	Uses phase and time encoding for secure key exchange	Qiskit, QuTiP	Optical setups, Multiple qubits	Phase and time encoded qubits, qubit measurements
Four-State QKD [38]	QKD protocol based on four non-orthogonal states	Qiskit, QuTiP	Optical setups, Single qubit	Qubits in four non-orthogonal states, qubit measurements
COW QKD [39]	Continuous wave QKD protocol	Qiskit, QuTiP	Optical setups, Continuous wave	Continuous wave quantum signals, homodyne measurements
Decoy-State QKD [40]	Utilizes decoy states for enhanced security	Qiskit, QuTiP	Optical setups, Single qubit	Qubits with decoy states, qubit measurements
SARG 04 QKD [41]	QKD protocol using four mutually unbiased bases	Qiskit, QuTiP	Optical setups, Single qubit	Qubits with four mutually unbiased bases, qubit measurements
Modified BB84 [42]	Enhanced version of BB84 with additional security	Qiskit, QuTiP	Optical setups, Single qubit	Random bit sequences, photon polarization states
Twin-Field Phase-Time [43]	Combines twin-field QKD with phase-time encoding	Qiskit, QuTiP	Optical setups, Multiple qubits	Phase and time encoded qubits, qubit measurements
Proposed Model	Description of the proposed model	Python, Qiskit, QuSim, QuTiP	Optical setups, Multiple qubits	Phase and time encoded multi-qubits, multi-qubit measurements

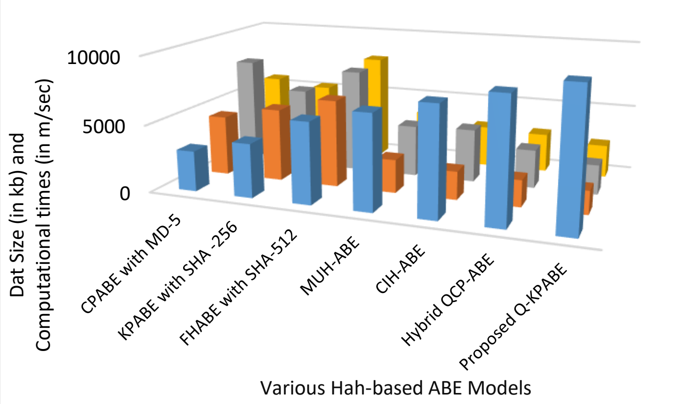


FIG. 3. COMPARATIVE ANALYSIS OF HASH-BASED ABE STANDARDS.

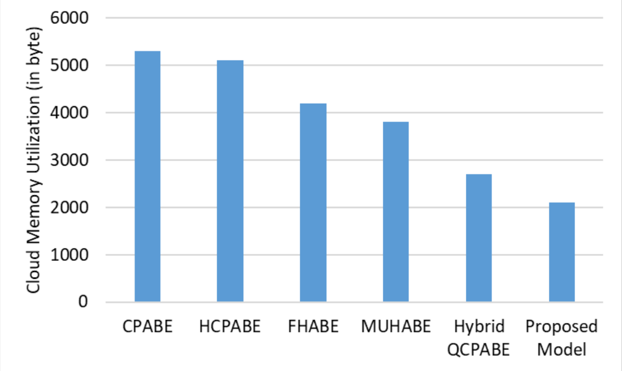


FIG. 4. THE RELATIVE STUDY OF MEMORY USAGE OF ABE STANDARDS.

Additionally, the study focused on multimedia data kinds, thus future research could apply the proposed approach to other data types. Future studies could integrate the proposed technique with encryption, access control, and authentication. This connection could improve cloud data security. Fig. 3 compares hash-based encryption techniques for 1 GB cloud consumer data. SHA-2, SHA-1, MD-5, and MD-4 hash algorithms are used to compare CP-ABE, KP-ABE, and FH-ABE. The computation takes milliseconds. The results showed that the planned standard computes 28% faster than existing standards. Even with 1GB of data, the multi-qubit QKD CPABE model utilizes less cloud server capacity than standard models, as shown in Fig. 4. These findings show that the proposed standard can better use cloud resources regardless of data amount. Fig. 5 compares the processing speed of the planned and traditional models. When processing 1 GB of data, the suggested standard took much less time than traditional methods. Figure 6 shows computational time comparisons for dynamic randomized session-wise key generation standards. Existing models take longer to compute dynamic randomized session-wise key generation than the suggested model.

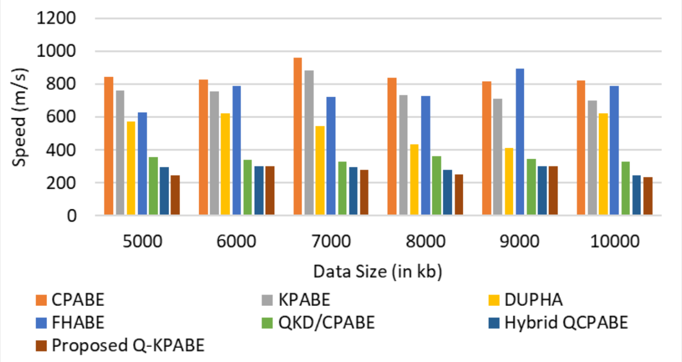


FIG. 5. COMPARISON OF THE AVERAGE COMPUTATIONAL TIME OF DIFFERENT MODELS BASED ON 1GB OF INFORMATION.

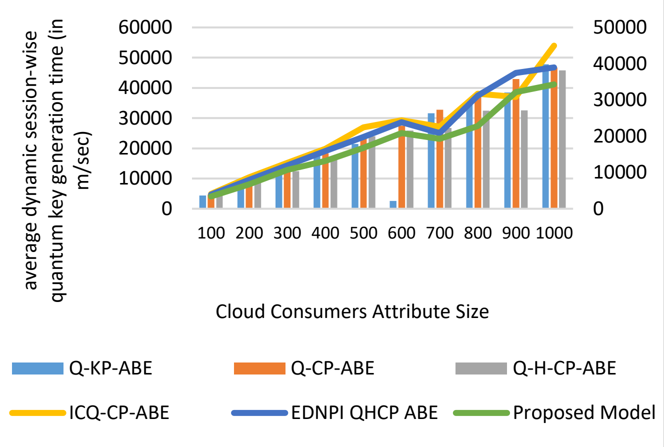


FIG. 6. COMPARISON OF VARIOUS STANDARDS AVERAGE DYNAMIC SESSION-WISE QUANTUM KEY GENERATION TIME WITH THE ATTRIBUTE SIZE.

V. CONCLUSION

The proposed multi-qubit QKD CP-ABE technique has proved that it secured cloud data with minimum computational overhead as compared to the existing models. The investigation showed that the suggested paradigm secures cloud-based data, improves performance, and reduces computing time and space. The proposed standard fragments the owner's data and distributes it to cloud servers. Based on their admission rules and a signature, the cloud information provider grants access to the intended user. Merging the decrypted text yields the original data. In order to assess its security, this study will deploy the suggested model in real-world cloud-based IoT and IIoT platforms. The proposed model can also handle cloud-based large data computing with great security. Quantum security models for cloud data are still in development, thus additional study is needed. This model and other quantum-based security models are likely to become more widely used and incorporated into cloud-based applications and systems, delivering more secure and efficient data protection solutions as quantum technology evolves. The study proves that quantum-based security models can improve cloud security and establish the framework for future research. Multi-qubit QKD CP-ABE and quantum mechanics secured cloud data. Cloud servers fragment data and allow access based on signature-verified admission rules. Future research will use secure cloud-based big data processing on IoT and IIoT platforms. Research is needed on quantum security models. Quantum technology improves cloud security, study finds.

The practical implications of our multi-qubit Quantum Key Distribution (QKD) model for end-users and real-world applications are investigated. Our use cases show how our model's security and efficiency benefit consumers distinctively. Enhancing Cloud Data Security, Cloud data security is improved by our multi-qubit QKD encryption key exchange standard. CP-ABE creates keys, encrypts and decrypts data, and securely shares keys. Figure 1 shows how administrators authenticate and store user data for restricted access. Possible Use Strong security is needed for personal data, internet banking, financial transactions, confidential company data, and government and military applications. Remote business and internet meetings require secure video conferencing. Video conference confidentiality is feasible with our model. The quantum key distribution system securely transfers encryption keys, making eavesdropping impossible. Our technology safeguards artists', authors', and creators' cloud-stored IP. Filmmakers can save their unreleased films in the cloud and restrict distribution to authorized distributors. These examples demonstrate how our multi-qubit QKD technique affects end-users in various industries. In real-world applications, its increased security, efficient encryption, and attribute-based access control protect important data. Our model beats existing QKD models in key generation rate, transmission distance, computing time, server space utilization, and security strength, which may affect end-users and cloud data security.

TABLE VI: GLOSSARY OF KEY TERMS AND CONCEPTS

Term	Definition
CP-ABE	Ciphertext-Policy Attribute-Based Encryption is an encryption scheme that grants data access based on attributes and conditions rather than explicit key exchange.
Cloud-Based Simulators	Software tools or platforms hosted in cloud environments for simulating various processes, such as quantum cryptography scenarios.
Dynamic Key Production	The generation of cryptographic keys on-the-fly for securing data communication.
Hash Techniques with Randomization	Methods that introduce unpredictability into cryptographic processes, enhancing security.
Hilbert Space	A mathematical space used to describe the state of quantum systems, represented as complex vectors.
No-Cloning Principle	A fundamental concept in quantum mechanics, stating that creating an exact copy of an arbitrary unknown quantum state is impossible.
Quantum Key Distribution	A quantum cryptography technique to securely generate and distribute cryptographic keys between two parties.
MDI -QKD	Measurement-Device-Independent QKD is a protocol that ensures security even if the measurement devices are untrusted.
Quantum No-Clone Theorem	A foundational principle stating the impossibility of creating an identical copy of an arbitrary quantum state.

ACKNOWLEDGMENT

The authors acknowledge the Researchers Supporting Project number (RSP2023R34), King Saud University, Riyadh, Saudi Arabia.

REFERENCES

[1] Cheng, H.; Li, J.; Lu, J.; Lo, S.-L.; Xiang, Z. Incentive-Driven Information Sharing in Leasing Based on a Consortium Blockchain and Evolutionary Game. J. Theor. Appl. Electron. Commer. Res. 2023, 18, 206-236.

[2] Diaconita, V.; Belciu, A.; Stoica, M.G. Trustful Blockchain-Based Framework for Privacy Enabling Voting in a University. J. Theor. Appl. Electron. Commer. Res. 2023, 18, 150-169.

[3] Islam, M. M.; Nooruddin, S.; Karray, F.; Muhammad, G. Internet of Things: Device Capabilities, Architectures, Protocols, and Smart Applications in Healthcare Domain. IEEE Internet of Things Journal, 2023, 10(4), 3611-3641.

[4] Muhammad, G.; Alhussein, M. Security, Trust, and Privacy for the Internet of Vehicles: A Deep Learning Approach," IEEE Consumer Electronics Magazine. 2022, 11(6), 49-55.

[5] Waters, B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. Public Key Cryptography–PKC 2011: 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011.

[6] Lee, C.-C.; Pei-Shan, C.; Hwang, M.-S. A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments. Int. J. Netw. Secur. 2013, 15(4), 231-240.

[7] Ibraimi, L. et al. Efficient and provable secure ciphertext-policy attribute-based encryption schemes. Information Security Practice and Experience: 5th International Conference, ISPEC 2009 Xi'an, China, April 13-15, 2009.

[8] Cheng, Y. et al. Efficient revocation in ciphertext-policy attribute-based encryption based cryptographic cloud storage. Journal of Zhejiang University SCIENCE C. 2013, 14(2), 85-97.

[9] Kumar, P.; Alphonse, P. J. A. Attribute based encryption in cloud computing: A survey, gap analysis, and future directions. Journal of Network and Computer Applications. 2018, 108, 37-52.

[10] Nuttapong, A.; Yamada, S. Duality in ABE: converting attribute based encryption for dual predicate and dual policy via computational encodings. Topics in Cryptology–-CT-RSA 2015: The Cryptographer's Track at the RSA Conference 2015, San Francisco, CA, USA, April 20-24, 2015.

[11] Lin, H., et al. Secure threshold multi authority attribute based encryption without a central authority. Information Sciences. 2010, 180(13), 2618-2632.

[12] Zukarnain, Z. A.; Khalid, R. Quantum key distribution approach for cloud authentication: Enhance tight finite key. International Conference on Computer Science and Information Systems (ICSIS'2014). 2014, Dubai, UAE.

[13] Gabriel, A. J., et al. Post-quantum cryptography based security framework for cloud computing. J. Internet Technol. Secur. Trans.(JITST). 2015, 4(1), 351-357.

[14] Khalid, R.; Zukarnain, Z.A. Cloud computing security threat with quantum key distribution defense model. Proc. of the 3rd International Conference on Green Computing, Technology and Innovation (ICGCTI2015). 2015, Selangor, Malaysia.

[15] Sharma, G.; Sheetal, K. A novel scheme for data security in cloud computing using quantum cryptography. Proceedings of the International Conference on Advances in Information Communication Technology & Computing. 2016, Bikaner, India.

[16] Shih, H.; Lee, K.; Hwang, T. New efficient three-party quantum key distribution protocols. IEEE J. Sel. Top. Quant. Electron. 2009, 15, 1602–1606.

[17] Masud, M.; Gaba, G. S.; Choudhary, K.; et al. Lightweight and Anonymity-Preserving User Authentication Scheme for IoT-based Healthcare. IEEE Internet of Things Journal, 2022, 9(4), 2649-2656.

[18] Cotler, J.S.; Shor, P.W. A New Relativistic Orthogonal States Quantum Key Distribution Protocol. Quantum Information & Computation. 2014, 14, 1081–1088.

[19] Gao, F.; Qin, S.-J.; Guo, F.-Z.; Wen, Q.-Y. Dense-Coding Attack on Three-Party Quantum Key Distribution Protocols. IEEE Journal of Quantum Electronics. 2011, 47(5), 630-635.

[20] Chuan, W.; Wan-Ying, W.; Qingand, A.I.; Gui-Lu, L. Deterministic Quantum Key Distribution with Pulsed Homodyne Detection. Commun. Theor. Phys. 2010, 53, 67, 67–70.

[21] Wang, L.J. et al. Experimental authentication of quantum key distribution with post-quantum cryptography, npj Quantum Information. 2021, 7, 67.

[22] Lim, C.C.W.; Portmann, C.; Tomamichel, M.; et al. Device-Independent Quantum Key Distribution with Local Bell Test, Phys. Rev. X 3, 031006, 2013, 1–11.

[23] Huang, X.; Wijesekera, S.; Sharma, D. Agent-Oriented Novel Quantum Key Distribution Protocol for the Security in Wireless Network. Multiagent Systems, Intechopen. 2009, 261–277.

[24] Brougham, T.; Barnett, S.M.; McCusker, K.T.; et al. Security of high-dimensional quantum key distribution protocols using Franson interferometers. J. Phys. B: At. Mol. Opt. Phys. 2013, 46 104010, 1–14.

[25] Singamaneni, K.K. et al. An Enhanced Dynamic Nonlinear Polynomial Integrity-Based QHCP-ABE Framework for Big Data Privacy and Security. Security and Communication Networks, 2022, 4206000.

[26] Singamaneni, K.K. et al. An Efficient Hybrid QHCP-ABE Model to Improve Cloud Data Integrity and Confidentiality. Electronics. 2022, 11.21, 3510.

[27] Singamaneni, K.K. et al. A Novel QKD Approach to Enhance IIOT Privacy and Computational Knacks. Sensors. 2022, 22, 6741.

[28] Tamma, Lakshmi Naga Divya. "a quantum chaotic hash based attribute based encryption on data and storing in cloud." (2020).

[29] Dowling, Jonathan P., and Gerard J. Milburn. "Quantum technology: the second quantum revolution." Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences 361.1809 (2003): 1655-1674.

[30] Wang, Jian, et al. "Research of hash-based secure key expansion algorithm for practical QKD." Optik 124.15 (2013): 2273-2276.

[31] Shor, Peter W., and John Preskill. "Simple proof of security of the BB84 quantum key distribution protocol." Physical review letters 85.2 (2000): 441.

[32] Ling, Alexander, et al. "Experimental E91 quantum key distribution." Advanced Optical Concepts in Quantum Computing, Memory, and Communication 6903 (2008): 69030U.

[33] Liu, Yang, et al. "Experimental twin-field quantum key distribution through sending or not sending." Physical Review Letters 123.10 (2019): 100505.

[34] Lo, Hoi-Kwong, Marcos Curty, and Bing Qi. "Measurement-device-independent quantum key distribution." Physical review letters 108.13 (2012): 130503.

[35] Kumar, Rupesh, Hao Qin, and Romain Alléaume. "Coexistence of continuous variable QKD with intense DWDM classical channels." New Journal of Physics 17.4 (2015): 043027.

[36] Wang, Shuang, et al. "Twin-field quantum key distribution over 830-km fibre." Nature photonics 16.2 (2022): 154-161.

[37] Molotkov, S. N. "Cryptographic robustness of a quantum cryptography system using phase-time coding." Journal of Experimental and Theoretical Physics 106 (2008): 1-16.

[38] Qu, Zhen, Ivan B. Djordjevic, and Mark A. Neifeld. "RF-subcarrier-assisted four-state continuous-variable QKD based on coherent detection." Optics Letters 41.23 (2016): 5507-5510.

[39] Stucki, Damien, et al. "Coherent one-way quantum key distribution." Photon Counting Applications, Quantum Optics, and Quantum Cryptography. Vol. 6583. SPIE, 2007.

[40] Lo, Hoi-Kwong, Xiongfeng Ma, and Kai Chen. "Decoy state quantum key distribution." Physical review letters 94.23 (2005): 230504.

[41] Mizutani, Akihiro, et al. "Measurement-device-independent quantum key distribution for Scarani-Acin-Ribordy-Gisin 04 protocol." Scientific reports 4.1 (2014): 5236.

[42] Chong, Song-Kong, and Tzonelih Hwang. "Quantum key agreement protocol based on BB84." Optics Communications 283.6 (2010): 1192-1195.

[43] Bialowons, Lucas, et al. "A Scalable Multi-User QKD Hub for Entanglement-Based Phase-Time Coding." Quantum Information and Measurement. Optica Publishing Group, 2021.

[44] Yang, Yu-Guang, et al. "Flexible protocol for quantum private query based on B92 protocol." Quantum information processing 13 (2014): 805-813.

[45] Lo, Hoi-Kwong, Marcos Curty, and Bing Qi. "Measurement-device-independent quantum key distribution." Physical review letters 108.13 (2012): 130503.

[46] Buttler, W. T., et al. "Practical free-space quantum key distribution over 1 km." Physical Review Letters 81.15 (1998): 3283.

Kranthi K. Singamaneni received his Ph.D. in Applied Cryptography and Cloud Security from GITAM Deemed to be University in 2020, Visakhapatnam, Andhra Pradesh, India. He received his M. Tech degree in Computer Science from Acharya Nagarjuna University, Guntur, Andhra Pradesh, India, in 2010. Also, he received his M. Tech degree in Information Technology from JNTU Kakinada, Andhra Pradesh, India in 2015. His research area includes Applied Cryptography, Network, and Cloud Security. He has about 17 years of experience in teaching, Industrial, and Research areas of Computer Science and worked as a Data Specialist at IBM. His Industrial experience includes Data Warehousing and Big Data Analytics tools. Dr. Singamaneni received a prestigious "Governors National Award for Excellence in Research and Development," GRA approved by the Ministry of Science and Technology for 2017-18. He is a member of ISTE, CSI, IFERP, and IAENG.

Ghulam Muhammad (Senior Member, IEEE) received a B.S. degree in computer science and engineering from Bangladesh University of Engineering and Technology, Dhaka, Bangladesh, in 1997, and an M.S. degree in knowledge-based information engineering in 2003, and the Ph.D. degree in electrical and computer engineering from Toyohashi University and Technology, Toyohashi, Japan, in 2006. He is a Professor at the Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. He holds two U.S. patents. His research interests include AI, machine learning, image and speech processing, and smart healthcare. Prof. Muhammad was a recipient of the Japan Society for Promotion and Science fellowship from the Ministry of Education, Culture, Sports, Science and Technology, Japan.

Zulfiqar Ali (Member, IEEE), Zulfiqar Ali received M.Sc. and M.S. degrees in computer science from the University of Engineering and Technology Lahore, Pakistan in 2007 and 2010, respectively, and obtained Ph.D. degrees in electrical and electronic engineering from the University of Technology Petronas, Malaysia in 2017. He is currently working as a Lecturer in the School of Computer Science and Electrical Engineering, University of Essex, Colchester, UK. His current research interests include explainable AI, digital speech and image processing, privacy and security in healthcare using watermarking, and audio forgery detection. Dr. Ali is a Fellow of the Higher Education Academy, Advance HE, UK.