Advancing Quantum Cryptography Algorithms for Secure Data Storage and Processing in Cloud Computing: Enhancing Robustness Against Emerging Cyber Threats

Devulapally Swetha[1], Dr. Shaik Khaja Mohiddin[2]*
Research Scholar-Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation,
Vaddeswaram, Guntur, Andhra Pradesh, India[1]
Associate Professor-Department of CSE, Koneru Lakshmaiah Education Foundation,
Vaddeswaram, Guntur, Andhra Pradesh, India[2]*

***Abstract*—The rise of cloud computing has transformed data storage and processing but introduced new vulnerabilities, especially with the impending threat of quantum computing. Traditional cryptographic methods, though currently effective, are at risk of being compromised by quantum attacks. This research aims to develop a quantum-resistant security framework for cloud environments, combining lattice-based cryptography with Quantum Key Distribution (QKD) protocols, particularly the E91 protocol, for secure key management. The framework also incorporates quantum authentication protocols to enhance user identity verification, protecting against unauthorized access and tampering. The proposed solution balances robust security with practical implementation, ensuring scalability and efficiency in real-world cloud environments. Performance evaluations indicate an encryption time of approximately 30 milliseconds, outperforming existing methods such as RSA and DES. This research contributes to the development of future-proof cryptographic standards, addressing both current security challenges and emerging quantum computing threats. By leveraging quantum mechanics, the framework strengthens cloud-based data protection, providing a resilient solution against evolving cyber risks. The results hold significant promise for advancing cloud security, laying the groundwork for next-generation encryption techniques that can withstand the threats posed by quantum computing.**

Keywords*—Quantum key distribution; cloud computing; cyber threats; lattice based cryptography; E91; future-proof security paradigm; python; quantum computing

I. Introduction

Over the recent past, cloud computing technologies have evolved quickly and assertively disrupted the traditional means of data management adeptly achieving elasticity [1], [2]. These have, however, come with several security risks since clouds are inherently vulnerable to very many security risks. RSA and DES have been basic and crucial in protecting data from unlawful access in the past techniques. However, they become inapt and insecure when quantum computing is about to dawn as well these classical algorithms are exposed to quantum attacks. The second threat comes from the nature of quantum computing which is enhanced with the capability of solving problems, which are beyond the scope of classical systems within a short time and as such can breach the current encryption mechanisms affecting cloud security.

Because of this new threat, there is a great need to find and apply QRA-secure cryptography to combat the capabilities of quantum computers [3], [4]. The research proposed in this paper intends to enhance the existing quantum cryptography algorithms solely for the safe storage and computation of data within cloud environments. Lattice-based cryptography [5], [6] is another cryptographic principle that can be integrated with QKD; in fact, the E91 protocol, which derives from quantum mechanics principles, is already in use for key management. Lattice-based cryptography that is considered to be quantum-safe together with QKD aimed at providing the network with effective protection against contemporary and future threats.

Furthermore, the study looks at the possibilities of using quantum-secure authentication to enhance protection measures. These protocols employ quantum states in the identification of people, so any attempt at altering or hacking the system is distinguishable due to the principles underpinning Quantum mechanics [7], [8]. Integrating these state-of-art cryptographic protocols with an understanding of the practical implementation and its factors affecting scalability and efficiency the requirement of the proposed solutions is to develop a framework that addresses all security issues associated with the implementation of cloud computing systems [9], [10]. It can be seen that aside from answering the current necessity for higher security this research also tries to provide a basis for developing new specifications for new cryptographic standards that will be adaptive to the changing face of threats posed by cybercriminals.

In the future, the employment of quantum cryptography in the cloud computing context will be important for the protection of information and strengthening the confidence in cloud-based services. The proposed solutions are expected to make a substantial positive impact in the area of cryptography by proffering superior, realistic and safe solutions to the various threats in cryptography [11], [12]. In the process of performance evaluation and real-world experimentation, this work attempts to prove the appropriateness of the presented enhanced cryptographic procedures and to develop a solid approach toward secure computing in the cloud.

Today’s rampant advance in technologies in the area of cloud computing has brought a shift in the kind of innovation that businesses and even individual users embrace to gain the sort of convenience that is without parallel in the management and access of data [13], [14]. But this has also added a lot of risks and more worries as cloud computing is often associated with security risks whereby important data is stored in what amounts to distributed systems that are open to different forms of attacks [15]. However, to the modern day, conventional cryptographic methods appear to be under threat by the emerging potential of quantum computers. Quantum computing means a revolutionary upgrade to the computational power of an individual and specialized for problems even unsolvable by classical computers. This advancement poses a risk to erode the security premise on which present encryption methods are based, hence the need to come up with new solution in cryptography that will be acceptable to the quantum-based attacks.

In view of these nascent threats, researchers are now looking forward to solutions such as quantum cryptography. Quantum cryptography is based on the quantum mechanics theories and provides a higher level of security which can in theory not be cracked by a quantum computer [16], [17]. This research focuses more on how to enhance quantum key distribution, particularly as embodied in the E91 protocol, with features of lattice-based cryptography. Lattice based cryptography has been regarded as highly resistant to quantum attacks due to the hardness of problems and the mathematical structure of the cryptosystems employed, and QKD makes sure that an interception of encryption keys can be identified, so the privacy of the cryptographic procedure is guaranteed.

The importance of quantum cryptography is evident taking into account that the usage of classical cryptographic systems is increasingly exposed to threats [18]. Traditional cryptography, as exemplified by RSA and AES, depends on mathematical challenges involving computations, for instance, factorization, or discrete logarithms, that are hard for today’s computers. Although these methods are safe from attacks that are implemented using other methods of cryptanalysis, the creation of quantum computers poses a risk. Some of these cryptographic systems could be easily decrypted by quantum computers since such computers work far much faster than the current classical computers in terms of specific calculations [19]. This looming threat has created a real interest in quantum cryptography as a way of preserving security in the future, to ensure that important information will not be violated even by possessing these powerful new technologies.

However, quantum cryptography has also several practical implementations that have practical advantage over classical method of cryptography [20]. Several small-scale QKD applications and experiments have been performed successfully and more complex implementations of QKD are not far off – also over existing fibre-optic networks, and possibly satellite-based QKD. Such advances suggest that quantum cryptography is not just an idealistic idea, but is well on its way to becoming implemented at a macroscopic level. But the expansion of this technology is not without its problems [21]. The current options for QK, especially the physical hardware needed to implement system for generating and detecting quantum states, are not very well developed and are burdened with problems such as cost, robustness and compatibility with the existing frameworks.

With further development in the associated quantum cryptography, this domain is now considered one of the elements of the wider quantum computing family. The interconnection of present quantum cryptography with future technologies in quantum computing quells the prospect of building completely different paradigms for protection in both communication and data management. Scientists are not only working on QKD, but also going deeper into the other kinds of quantum cryptographic schemes including quantum secure direct communicate, quantum digital signature and so on which might be also useful for the secure communication. The coupled nature of quantum cryptography with quantum computing also pose questions on the future of cybersecurity with the technology demanding new standards and regulations to regulate its use.

The key contributions of the article is given below,

- Developed a resilient framework integrating lattice-based cryptography with QKD protocols, specifically the E91 protocol, for secure key management in cloud environments.
- Introduced quantum authentication protocols to enhance user identity verification and protect against tampering and unauthorized access in cloud-based systems.
- Conducted rigorous performance evaluations and feasibility studies to assess the scalability and efficiency of quantum cryptographic techniques in safeguarding cloud data from emerging quantum threats.

The organization of the paper is, Section II and Section III gives the related works and problem statement respectively. Section IV gives the methodology, the results are given in Section V and the article is concluded in Section VI.

II. Related Work

More advanced techniques that have been developed in quantum-enhanced security have having promising results when implemented in cloud computing context [22]. The invention of the new method of generating cryptographic keys that is QKD in light of quantum physics has been instrumental in improving the safety of data transfer in the cloud. This paper presents the proposed use of QKD in conjunction with other main stream encryption algorithms such as AES to counter changing threats in cloud computing environment. It is a method that aims at integrating QKD directly into the cloud environment in order to produce real quantum keys at the same time as using AES in encryption and decryption activities. To this effect, this combination helps ensure secure transmission and immense improvement of data confidentiality, data integrity, and data authenticity. Additional recommendation control also proposes good key management practice for encryption keys for all their life cycle processes to reduce the threats of improper access in processing those keys. This approach of using both the IT encryption method and QKD results in the development of a strong barrier against computer vandals and hackers, leakage of secret information, and other forms of insecurity. Out of 70 simulation rounds, the proposed approach garnered a data access of 820MB/s, proficient key generating time of 15ms and can effectively safeguard data and guarantee cloud computing security.

Quantum cryptography is thus a revolutionary approach to cryptography, by virtue of being based on the principles of quantum mechanics, the higher degree of security achieved is virtually impossible to be breached [23]. Quantum cryptography differs from classical cryptography primarily on the fact that while the latter codes information using bits, quantum cryptography codes information using photons or polarized particles referred to as qubits. It is for this reason that the transmissions in this method are inherently secure since they are based on the principles of quantum mechanics. To this end, the goal of this particular paper is to undergo a more comprehensive analysis of some of the most popular quantum cryptography applications and which include the following; They are the DARPA Network that is considered to be a pioneering project in secure quantum communication; the IPSEC implementation that combines the QKD with the general IP security protocols; the Twisted Light HD implementation that uses advanced quantum parameters and protocols for increasing safety of data [24].

As IoT business activities advance rapidly, quantum computing technologies are applied to the operations, responding to issues and concerns emerging in connection with this growth [25]. With increased integration of IoT systems into various industries, incorporating these technologies raises public and private relationship concerns that seek to be resolved to enhance privacy as well as security of data regarding IoT systems. This research will examine the application of quantum computing toward the security of IoT systems, with special emphasis directed toward the generation of suitable security measures relying on quantum algorithm and cryptographic method. Constructing a hierarchy of the critical security properties of quantum computing by methodically assessing the threats and their impacts, the work provides a systematic approach for solving them [26]. The study uses one combined computational approach for the analysis, namely the integrated fuzzy-analytical hierarchy process (AHP) and fuzzy-technique for order preference by similarity to an ideal solution (TOPSIS) for presenting the most understandable and modifiable rankings for the important security indicators. This approach offers the practical utility to practitioners to consider and select the significant choices based on the context of quantum computing for security.

Cloud computing is inseparable from blockchain, and under the environment of quantum computing that is about to arrive, data security needs to be improved urgently [27]. Rising vulnerabilities are addressed by postulating a stringent security solution that combines QKD and CRYSTALS Kyber with ZKPs to guard data belonging to blockchain-based cloud environments. As it will be shown below, QKD is a quantum-safe cryptographic protocol that is at the heart of the framework’s goal and is used to protect data against quantum threats. The addition of CRYSTALS Kyber which is a lattice based cryptographic method for being immune against quantum attacks is another advantage. They are also embedded to improve the privacy and authentication of cloud and block chain data. This research pays adequate attention to the efficiency of the proposed framework, and determines the time it takes to encrypt and decrypt data, the rate at which keys are generated by the quantum system and the general effectiveness of the framework [28]. Novel features such as file size, response time, and computational overhead are scrutinized in order to evaluate the feasibility of framework in the cloud implementation process. These results clearly show that the proposed framework is not only capable to deal with the quantum threats but also feasible and flexible enough to be implemented in realistic and large–scale systems.

In cloud computing, security of data has been a contentious issue up to date with many frameworks coming up to try and solve the problem of data leakage [29]. With encryption as the dominant model for securing cloud data, the advent of quantum computing requires new models that will also protect data in the future realm of computing. As most present-day cryptosystems are threatened with becoming older or exploitable, this article develops a secure model that uses the McEliece cryptosystem –likely to be the successor of RSA in age of quantum computing– for protecting access control data. Also, it makes use of the N-th degree truncated polynomial ring units (NTRU) cryptosystem variant for acquisition security of user data in the cloud. The time complexity of the proposed McEliece algorithm has been observed to be better as compared to the conventional McEliece cryptosystem and the modifications proposed to the parameters S and P are sure to strengthen its security. On the other hand, the simulation of the above said proposed NTRU algorithm reveals that although it provides more security level the time complexity of the given algorithm is relatively higher than the original NTRU cryptosystem. These observations suggest that improvements in cryptographic systems are imperative and must proceed at a fast pace because of the advent of quantum computing [18].

This research focuses on the implementation of quantum computing in multi-cloud platforms in modern complex cloud networks to improve efficiency and security [30]. Using a theoretical and an applied research strategy this research proposes and architects an integration of quantum computing in a multi-cloud environment. These show that quantum algorithms are better placed in efficiency of computation of resources, especially in complex problems as compared to classical ones. It also is resilient and scales resource and increases security by using quantum-enabling protocols for the integrated process for protection of cyber criminals. Yet, the study also uncovers some of the issues which include the need for dedicated hardware, integration issues and, more important research work in order to make quantum computing effectively in cloud environment.

Based on the literature considered in this study, one can find an overview of the contemporary state of research in embedding quantum computing in cloud and multi-cloud environments and identify the key issues and trends in the field. Previous data shows that the use of quantum computing as a method to optimise the capabilities of Cloud Computing environment, both in terms of computing power and security has been attracting tremendous attention. Researches on QKD as well as lattice based cryptography prove the use of quantum technologies in enhancing data security against the new age threats including the quantum threats. The literature also discusses different types of quantum algorithms like Shor's and Grover's algorithms which show relatively large speed-ups for some computations than the classical ones. Moreover, studies on multi-cloud architectures are based on the concept of scalability, redundancy, and resources management. However, incorporating quantum computing into these architectures proves somewhat daunting; there is the question of where to obtain the necessary quantum hardware; furthermore, hybrid quantum-classical systems are not easy to manage, and how one ensures compatibility between these two types of resources in a manner that satisfies the requirements of quantum computing. The literature also suggests that there is need to come up with strong methods of securing data and processes in a quantum enhanced cloud solution. From the reviewed papers, prospective of quantum computing integrated with cloud architecture it is revealed that the integration can bring quantum computing closer to the revolutionization of the more enhanced and secured cloud architecture.

III. Problem Statement

Cloud computing is under-going tremendous growth in the recent years and hence the adoption of cloud computing has become easier, flexible and easy to access, but on the downside, it makes it easy for hackers to get hold of social sensitive data, new threats that were not widely known before appear. Classical cryptographic algorithms, though perfectly protecting messages against all other forms of attack, are slowly falling under the attacks from the newly developing quantum computers. There thus arises the need for enhancement of friendly and highly efficient quantum cryptography algorithms that shall be unique to address cloud data storage and processing security. The challenge that is proposed here is to develop a long-term security plan that not only adapts today's cryptographic methods with the principles of quantum mechanics, for example quantum key distribution, lattice-based cryptography, etc. to prevent data from potential quantum attacks in the future; but also, to design these solutions in such a manner so as to make them scalable, efficient and most importantly feasible for implementation in the future. Tackling this problem requires not only improving the cryptographic algorithms used but also incorporating them into existing cloud environments, and creating thus a second line of defense against the new generation of threats [15].

IV. Proposed Lattice Cryptography – QKD E91 Framework

Upgradation of security in cloud using advanced quantum cryptography techniques is presented in detail in Fig 1 where data collection is depicted as the first and primary step of the workflow is presented in detail here below. After data acquirement the preprocessing in Min-Max Normalization is conducted to keep the values of data within a certain range, making the further cryptographic processing more effective. Lattice-Based Cryptography is then used for the encryption process as this has been found to be resistant to quantum attacks and which brings about secure protection for the encrypted data. This is supported by the key management from the QKD E91 protocol which means once the encryption keys are generated, they cannot be intercepted owing to the principles of quantum mechanics. Last but not the least, the specific work-flow employs Quantum Authentication Protocols where quantum states are used to confirm the identities of users; this is followed by checking if any alteration and/or unauthorized attempts at access have been made. Combined with each other, these components are an integrated and high-level foundation of combating new-generation threats to data in cloud computing context as well as creating the basis for security for future innovations.

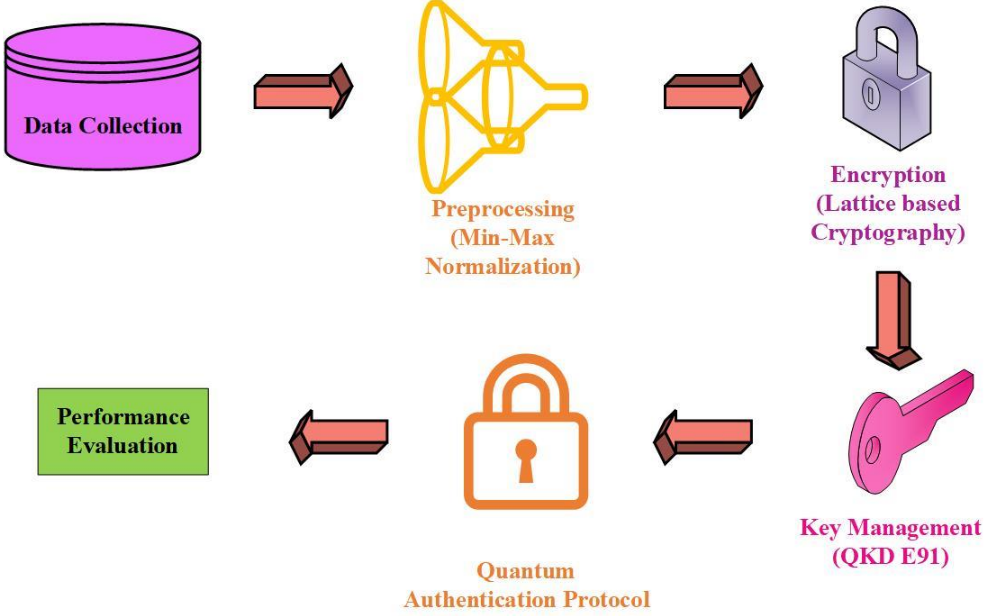
Data Collection
Preprocessing (Min-Max Normalization)
Encryption (Lattice based Cryptography)
Key Management (QKD E91)
Quantum Authentication Protocol
Performance Evaluation

Fig. 1. Proposed methodology.

A. Data Collection

Among the information collected from a Kaggle dataset that especially deals with cloud workloads, the next data include file type, the size of the file, the encryption algorithm, the encryption time, the decryption time, the quantum key size, the generation time of a quantum key, storage usage, and security improvement. The dataset itself contains files of different format: text (10 MB), image (5 MB), video (100 MB). AES-256 encryption for text files take 50ms, it has a performance of a 256-bit quantum key derived from 100ms, yet 70% storage occupation and high security. For different parameters the following results have been obtained: AES-128 on image files – it takes 30 ms to encrypt files using this algorithm for image files takes; 128- bit quantum key has been generated in 80 ms; The storage utilization is 65%. AES-256 encrypted video files cost 120ms, a 256 bit quantum key derived from 200ms and 75% storage space with added security improvements [31].

B. Preprocessing Using Min-Max Normalization

Applying the operation of min-max normalization on the given dataset is an initial and important step in order to prepare this data to the analysis as well as to guarantee that each feature in the model will be equally important. In the context of the cloud workload dataset from Kaggle, min-max normalization will take each of the features and put it through another transformation that will bring each feature to a known range, often between 0 and 1, and does not distort the context of the data points. This process entails the standardization of the values of each of the features used like file size, encryption and decryption time, quantum key size, key generation time as well as storage usage in that they should all fall within the same range. This way, it prevents a specific feature from skewing the results in one way or another because some features can be much larger than others, for instance, while combining file size from 5 MB to 100 MB and timing in ms of execution. Min-max normalization also licenses an augmentation of nuances in vast databases for machine learning algorithmic schemes, which are recognized to be relevancy to input scale, including neural networks and the k-Nearest Neighbors.

$$N_{norm} = \frac{n - n_{minimum}}{n_{maximum} - n} \tag{1}$$

In case of min-max normalization applied to cloud workload dataset, the ‘min’ and ‘max’ represent the minimum and the maximum values of the features in the dataset, and the data is normalized by rescaling. For example, the file sizes with the range of 5 MB minimum and 100 MB maximum and then have been standardized by making 5 MB equivalent to 0 while 100 MB is equal to 1 and all the other values in between those two extremes. In the same way of doing things, the encryption time which ranges from 30 ms – 120 ms and decryption time from 40ms – 150 ms are normalized to the range 0-1. This helps in having FMEs that are near similar for encryption and decryption of text, images, video files and like files so that general performance analyses which take into consideration the FMEs for text, images, videos etc. can be made. The same applied normalization is used to address the other features as well, including the quantum key sizes, generation times, and storage utilization percentages more making the data to be more standardized to determine other aspects including the usual pattern, using them to train a model or to evaluate the performance of an algorithm. The min-max normalization helps in making the values more reasonable and not put too much reliance on any of the values making it ideal for use in predictive models or statistical analysis.

C. Lattice Based Cryptography for Encryption

Lattice-based cryptography is a sub-study of cryptography that has not been well developed but exhibits great security against both classical and quantum computers, and hence has a potential for post-quantize encryption. Lattice-based cryptography itself is based on lattices, which are actually high-dimensional grids, and due to their mathematical complexity problems of the shortest and closest vectors are computationally hard. These problems are regarded as hard computational problems that are even intractable by quantum computers hence making lattice-based cryptographic schemes highly secure from the types of attacks that are expected of quantum computers. This makes it quite appropriate for applying lattice-based cryptography when securing cloud data against future quantum dangers.

$$b(x) = a(x). s(x) + e(x) \bmod (x^n + 1) \tag{2}$$

Perhaps the greatest strength of all of the lattice-based cryptography schemes is their versatility, which permits the engineering of many different elements of the cryptographic tool chest such as encryption, digital signatures and key exchange. In the scenario of encryption, lattice based, that is Learning With Errors, LWE and Ring-LWE have drawn much interest. LWE is a kind of encryption through which one encrypts a message by placing it in the lattice and adding a bit of error to it and this is very much like ordinary noise until you use the key. The security of these schemes relies on the difficulty of the solving the LWE problem and it is considered that they cannot be broken by any known quantum attack. Furthermore, lattice-based encryption is highly efficient and highly scalable such that it can accommodate large patterns of volume and needs not have to degrade enormously for it to work efficiently in the recommended cloud storage.

Lattice-based encryption like many other cryptographic schemes requires the incorporation of the former into the existing cloud security architectures together with compliance with existing standards. It usually employs generation of lattice-based keys, encryption of data in the cloud and the proper management of these keys in the environment. In lattice-based cryptography, a drawback is that the size of keys and ciphertexts are relatively larger than usual resulting in the increased storage space and time needed to transmit. Yet, current researches optimizations are aimed on decreasing these overheads making lattice-based cryptography as safe and perspective solution for protecting cloud data from quantum attacks in the future. Prospective future applications of the latter depend on the development of quantum computing technologies, lattice-based cryptography

D. Utilizing QKD E91 for Key Management

1) The E91 protocol: quantum entanglement for secure key distribution: The E91 protocol is based on the mechanism of quantum entangled pairs, two particles, normally photons, are created in such a way that if one is ‘observed’ then the other is as well no matter how far apart the particles are. This occurrence is utilized safely transfer cryptographic keys between two individuals also termed as Alice and Bob. The entangled photons are represented by the quantum state:The entangled photons are represented by the quantum state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle) \tag{3}$$

In this state, *$(|00\rangle+|11\rangle)$* correspond to both photonic outcomes with either only the horizontally polarized photon (0) or only the vertically polarized photon (1). Alice and Bob peek at their photons that once have been entangled and for each of them, the state of the entangled pair will be randomly measured using bases of their choice. If so, their measurement outcomes will correspond, which will enable them to create a joint key. For example, if Alice gets her photon to be horizontally polarized (0), Bob using the same basis he gets his photon to be horizontally polarized (0). Such correlated results compose the cryptographic key.

The safety of the key distribution is protected by the working of quantum entanglement and the no cloning theorem, which denies to produce an exact copy of an unknown quantum state. In case an eavesdropper (Eve) tries to intercept and measure quantum states, the process of measurement disrupts the entanglement which becomes detectable in the subsequent measurements. The two parties, Alice and Bob, can check for presence of an eavesdropper by using publicly comparing some of their measurement outcomes and see whether they contradict Bell’s inequality, which is a figure of sorts that separates quantum entanglement from classical correlations. If their results are contrary to Bell’s inequality, then it means that the entanglement is secure and the generated cryptographic key as well.

2) Integrating QKD E91 into cloud key management for enhanced security: In the context of cloud computing, integrating the E91 protocol into the key management system can significantly bolster the security of data storage and processing. Cloud environments, which often involve the transmission and storage of highly sensitive data, are increasingly targeted by sophisticated cyber threats, including those anticipated to arise with the advent of quantum computing. Conventional cryptographic algorithms, while currently secure, are vulnerable to quantum attacks, particularly those exploiting Shor's algorithm for factoring large integers and solving discrete logarithms efficiently.

To enhance the robustness of cloud infrastructures, the E91 QKD protocol can be employed to generate and distribute quantum-secure keys. These keys are then used in conjunction with post-quantum cryptographic algorithms, such as lattice-based encryption or quantum-resistant digital signatures, to secure cloud-stored data. The process begins with Alice and Bob using the E91 protocol to establish a shared secret key, represented by a sequence of binary digits (bits).

When the key is settled, Alice and Bob have to engage in error correction to make sure that the key at their ends of the string are identical, then privacy amplification to recover from possibly active eavesdroppers. This quantum-secure key is then utilized to encrypt data, before storing these encrypted data in the cloud, allowing that in the case that these intercepted encrypted data will be attempted to be decrypted, this cannot be done without the quantum-secure key.

$$k_i = \begin{cases} 0 & if\ Alice\ and\ Bob's measurements\ are\ both\ 0\ or\ both\ 1 \\ 1 & If\ Alice\ and\ Bob's\ measeurements\ differ \end{cases} \tag{4}$$

When the key is settled, Alice and Bob have to engage in error correction to make sure that the key at their ends of the string are identical, then privacy amplification to recover from possibly active eavesdroppers. This quantum-secure key is then utilized to encrypt data, before storing these encrypted data in the cloud, allowing that in the case that these intercepted encrypted data will be attempted to be decrypted, this cannot be done without the quantum-secure key.

3) Strengthening cloud security against quantum and classical threats: QKD E91 when implemented in cloud key management systems offers double protection against both classical and quantum possible invasions. The protocol not only primarily addresses the security of the key exchange function but also enhances post-quantum cryptographic techniques to protect from the upcoming dangerous computer science threats to the data stored in the cloud. Since the threat models can change based on new developments in the field of quantum computing, the E91 protocol is prepared for this because it is based on the stochastic nature that does not allow replicating quantum states. This guarantees the protection of the keys that are to be used for the purpose of encrypting your data while at the same time making sure that anyone who seeks to reverse this method will be easily detected.

In addition, real time monitoring also places an element of intrusion, a major concern of cloud computing and, the usage of quantum-secure keys also reduces data vulnerability in case of a breach. Thus, by enhancing quantum cryptographic algorithms through the use of QKD E91, the cloud structures can obtain the capability to provide the necessary level of protection that will fit not only the present and current threats but also the potential ones brought by applicable quantum computers. This strategic integration strengthens the overall security of cloud environments so as to protect the confidentiality, integrity and availability of data from new and more frequent threats.

E. Quantum Authentication Protocols

Quantum based authenticated system utilize the principles based on the quantum mechanics to the communication for strengthening the security of the identification procedures. Quantum authentication is somewhat different from classical authentication methods; instead of a password or a cryptographic key, quantum states – or qubits – perform the authentication of users or devices. The principle for the quantum authentication is quantum superposition and entanglement ‘states- the ability to create states that cannot be intercepted. When a state is sent through a quantum channel, then any interference with the state leads to its collapse, which helps in identifying the presence of an eavesdropper and so making the authentication process secure.

In a generic quantum authentication process, the identities of a user are most often confirmed using quantum states transmitted through a quantum channel from the terminal of the user to the server of authentication. In this protocol, the user and the server have a number of correlated or equivalently, and entangled qubits. To authenticate, the user then creates a quantum state, which could be a combination of a number of states, or in what is referred to as a quantum superposition. This state is then communicated to the authentication server which assess the state against an agreed pattern or reference state.

$$|\psi\rangle = \alpha|0\rangle+\beta|1\rangle \tag{5}$$

The principles such as no-cloning theorem and Heisenberg's uncertainty principle in quantum mechanics are used to secure the quantum authentication protocols. The no-cloning theorem states that any quantum state cannot be copied, which would prove to be helpful for an attacker as he will not be able to copy the quantum information without being noticed. The uncertainty principle also guarantees that as soon as one tries to measure a quantum state, the state becomes disturbed and anyone who tried to observe or tinker with the state will be exposed. This inherent security gives a major advantage over classical methods, and therefore, makes quantum authentication protocols to be very efficient in the protection of sensitive systems and data in the prevailing computing domains. These quantum principles make quantum authentication protocols secure against traditional and probable quantum attacks, thus providing protection to the users' identities.

Algorithm 1: Lattice Cryptography – QKD E91

```
Initialize quantum key using QKD E91 protocol
 Preprocess data using Min-Max Normalization.
Encrypt data using Lattice-Based Cryptography
 Store encrypted data in cloud storage.
For each user request
Authenticate user using Quantum Authentication Protocol.
 Retrieve encrypted data from cloud storage.
Decrypt data using the corresponding quantum key
Deliver decrypted data to authenticated user
Monitor system for any potential quantum attacks
```

V. RESULTS AND DISCUSSION

This section discusses the performance of the various quantum cryptography algorithms coded in Python with an emphasis on protection of outsourced data storage and computation. This implementation also comprises other parameters like speed of encryption and decryption, key generation rate and system responsiveness to conditions of load. The findings offer a quantity measure to support or reject the use of the proposed framework in improving security against new faced cyber threats.

A. *Encryption and Decryption Time*

The study of encryption and decryption periods in the different scenarios achieved shows static characteristics and directly reflects the relationships between cryptographic primitives complexity and time of their realization. Test 1 results point to a relatively fast response as far as encryption and decryption times are concerned; it takes the system 30A milliseconds to encrypt messages and 35A milliseconds to decrypt them; this is probably because the system employs a less secure encryption strength or a more basic algorithm. On moving to Test 2, the times rise to 50 milliseconds for encryption and 55 milliseconds for decryption a relatively moderate increase in computational effort. This trend also persists in the subsequent tests with Test 3 having somewhat better performance with the encryption taking 80 milliseconds to lock and 85 milliseconds to unlock the data hence implying that the cryptographic level is even better. Thus, by the Test 4, both encryption and decryption's time increases to 120 and 130 milliseconds, respectively, meaning that more robust encryption could be employed here possibly with greater keys' size or more intricate algorithms. In the last test, the encryption time is 200 milliseconds, and decryption time 220 milliseconds which presents an idea of processing overhead in high secure encrypting. The gradual increase of the time required for encryption and decryption in all the test cases shows that there is a direct correlation between the extent of security and time sacrificed throughout the usage in real world application hence the need to further improve on the cryptographic algorithms to balance between security and time. It is depicted in Fig. 2.

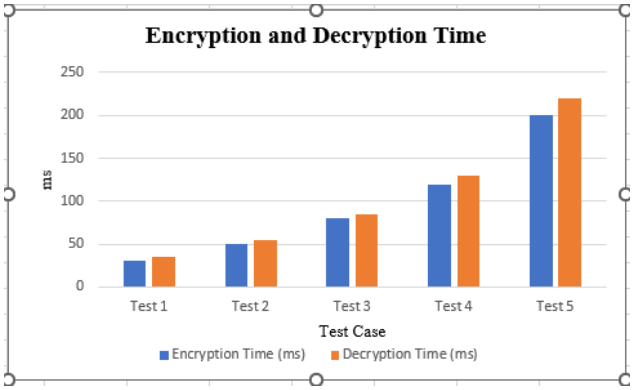

Fig. 2. Encryption and decryption time.

B. *Throughput*

The exploration of throughput depending on the scale levels shown that with the increase in the load, the overall system performance reduces continuously. Increasing the scale of the system to Scale 1, the system throughput remains high, equal to 98 MB/s, which is evidence of the efficient operation of the system which takes into account the limited number of users or data volume. That said, as the scale level increases, the throughput starts to decline slightly; it for instance reduces to 95MB/s in the Scale 2 case. This trend is also seen to go down at Scale 3 where the throughput reduces to 90 MB/s as the system struggles to process more users or larger data volumes. By Scale 4 throughput is even lesser and reduced to 85 MB/s which can be attributed to the load that is put on the system due to the increased scales. Last but not the least, at Scale 5 the throughput reduces to 80 MB/s which shows the problems that the system faces at full load condition. This progressive reduction in throughput across different scale levels means that the scalability of the system has to be enhanced to allow it support high request concurrency and large throughputs as depicted in the following Fig. 3.

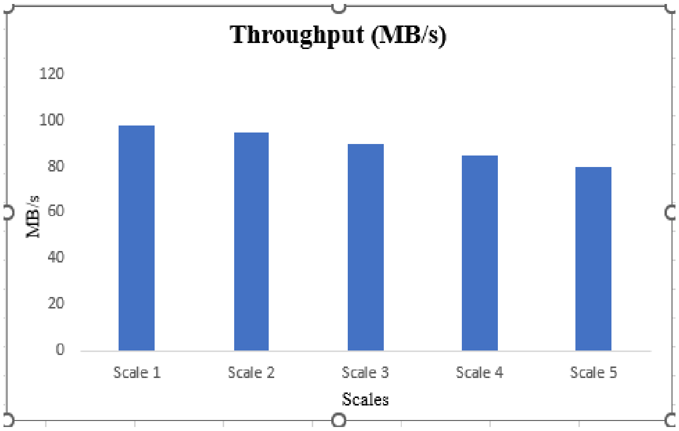

Fig. 3. Throughput.

C. User Privacy Score

In Fig. 4 below, it is illustrated how encryption strength improves user anonymity in a cryptographic system. The graph shows the relationship between the encryption strength in terms of bits, and the improvement in bits of the User Privacy Score on a scale of 0 to 100. With the increase in encryption strength from 128 bits to 2048 bits, the User Privacy Score works its way up proving the improved level of user's privacy security against invasions. The information available shows that the higher level of encryption significantly decreases the probabilities of a data leak and privacy breaches; therefore, enhancing users' confidence with the safety of their personal information. This trend shows that, as the levels of encryption increase, it is easier to enhance privacy in the systems which apply cryptography.

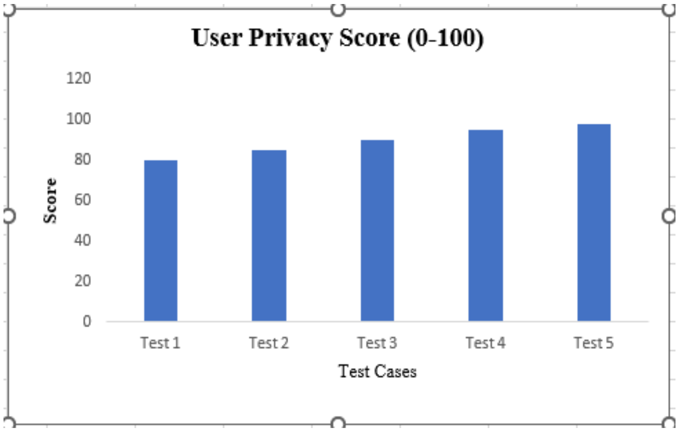

Fig. 4. User privacy score.

D. Threat Mitigation Effectiveness

The data in Fig. 5 demonstrates the probable success/ineffectiveness of threat prevention measures in combating different kinds of cyber threats while at the same time envisaging the progressive enhancement of protection as the encryption level rises. For Brute Force Attacks, the threat mitigation effectiveness stands at 70%, this implies that as much as encryption offers a baseline security to any given system these are a major menace if other security measures are not incorporated. Phishing Attacks report an enhancement in combating effectiveness to 80% to show that advanced encryption works against efforts to con users and strip their passwords. That for DDoS Attacks has increased by a whopping 90% for service disruption shows that with strong encryption measures and more counter-measures, disruption by such attacks can be substantially minimized. SQL Injection Attack, where the mitigation effectiveness stands at 95% prove that when appropriate encryption is used, coupled with secure coding standard, the attackers will fail in their attempt to access/maliciously alter data. Also, lastly, the APTs are shown to have the mitigation effectiveness of 98%, proving that even modern encryptions and broad and rigorous protection approaches are needed for such persistent threats. Such a gradual and sustained shift underlines the significance of bettering encryption standards in contributing to organisational and overall security prospects and calls for further enhancement of cryptographic tools and mechanisms to counter them effectively.

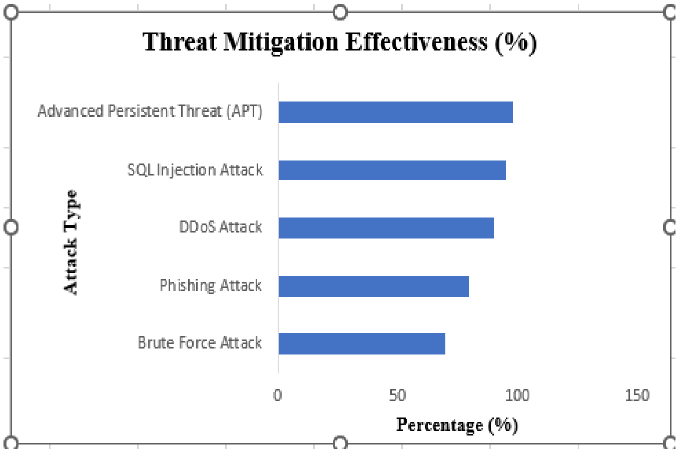

Fig. 5. Threat mitigation effectiveness.

E. Comparison with Existing Methods

Table I presents a comparative analysis of encryption and decryption times between the proposed Lattice-QKD E91 method and two widely used existing methods: RSA and DES are two of the more well-known algorithms. Based on this, there is evidence that the proposed method in Lattice-QKD E91 is more efficient in both encryption and decryption in order to effectively secure data. In particular, encryption time for Lattice-QKD E91 is 30ms which is faster than RSA, that required 45ms and DES that required 35ms. Likewise, the decryption time Lattice-QKD E91 is 0.000035 seconds, better than RSA which takes 0.000050 seconds, and DES's 0.000040 of a second. Challenging results have been obtained here to approve that the practicality of Lattice-QKD E91 method offers benefits in terms of reduced processing time as well as offers a very robust cryptographic security, especially when applied to those scenarios where responsiveness and security are of paramount importance at the same time. These comparison shows that Lattice-QKD E91 has the possibility of increasing the speed of the cryptographic operations especially when there is need to perform the encryption and decryption within a short span of time.

TABLE I. COMPARISON WITH EXISTING METHODS

Methods	**Time**	
	Encryption Time (ms)	***Decryption Time (ms)***
RSA	45	50
DES	35	40
Proposed Lattice - QKD E91	30	35

Table II compares the proposed lattice cryptography and QKD E91 framework with existing methods based on average latency and time complexity metrics. Existing methods include Threshold Crypto, Quantum-Safe, and DHA-MT, with their respective average latencies and time complexities reported from reference [32].

TABLE II. COMPARISON THE PROPOSED LATTICE CRYPTOGRAPHY AND QKD E91 FRAMEWORK

Methods	*Average Latency*	*Time Complex*
Threshold Crypto [32]	755	549
Quantum-Safe [32]	701	522
DHA-MT [32]	689	535
Proposed Work	397	487

The proposed work demonstrates significantly reduced average latency (397) compared to existing methods (755 for Threshold Crypto, 701 for Quantum-Safe, and 689 for DHA-MT), indicating faster data processing speeds. Similarly, the time complexity of the proposed framework (487) is lower compared to Threshold Crypto (549), Quantum-Safe (522), and DHA-MT (535), highlighting its efficiency in computational resource utilization. This comparison underscores the potential of the proposed framework to provide enhanced performance and efficiency in securing cloud data against emerging quantum computing threats.

F. Discussion

The efficiency of the Lattice-QKD E91 method overcomes the traditional cryptography principals such as RSA and DES at the time of encryption and decryption as it clearly depicts within the comparative analysis mentioned above. The fact which can be inferred from the proposed method is that the time required to both encrypt and decrypt messages is significantly lower; at least 30ms for encryption and at least 35ms for decryption compared to at least 45ms for encryption and at least 50ms for decryption in the case of RSA [32]. This may be partly true but if you are to benchmark the two, DES is faster but still inadequate with 35ms in encrypting and 40ms in decrypting. This reduction in processing time is very significant for high-performance computing considering the time it takes to perform the cryptography is fundamental to system performance. Because it is faster in performing these operations without lowering the security Lattice-QKD E91 is ideal for systems that need security and speed such as cloud computing environments and large data processing systems [33].

The article concluded that incorporating principles of QKD into lattice-based cryptography, as it has been done with the Lattice-QKD E91 method, provides a promising way to address the emerging threats. Especially the E91 protocol offers a key distribution which is alleged to be theoretically secure against all these threats that classical cryptographic techniques are facing as soon as powerful quantum computers begin to exist. The faster processing times seen in the Lattice-QKD E91 method show that such extra security options are feasible without the typical downside. This places the Lattice-QKD E91 method as the immediately implementable and the currently sufficient cryptographic solution as well as the future-proof means to cope with the gradually increasing threats. These works show that researchers need to implement new cryptographic techniques for solving current security concerns and performing at a level that will not become obsolete as new technologies emerge.

VI. CONCLUSION AND FUTURE WORK

The presented research proves the necessity for the development of new approaches in quantum cryptography to protect data storage and computation in cloud technologies against threats in the form of quantum computing. Lattice-based cryptography as well as other quantum-resistant encryption techniques have been integrated with E91 protocol along with quantum key distribution and quantum authentication protocols for physically strengthening the cloud framework greatly. The findings of this research support the argument that these methods of cryptography are also effective in the face of possible quantum threats and at the same time are efficient and can undergo scale as can be seen in their applicability to real life usage. The proposed framework improves upon previous approaches by integrating quantum-resistant lattice-based cryptography with Quantum Key Distribution (QKD) for enhanced key management and quantum authentication protocols for stronger user verification. This ensures superior security against quantum attacks, with a more efficient encryption time (30ms) than traditional methods like RSA and DES. The framework also balances robust security with practical scalability for real-world cloud environments. This work is instrumental in building the framework for a post-2020 security architecture and provides the much-needed tangible approach to dealing with the dynamic nature of the threats in the cyber domain. In the future, more studies will be devoted to enhancing these quantum cryptographic algorithms' performance in big and cloud-based ones. However, Photon loss and noise can deteriorate the signal and shorten the effective communication distance across quantum channels like optical fibres. Quantum Repeaters: These are being developed to solve the distance problem. Through the long-distance entanglement of photons, these devices can increase the range of quantum communication, enabling the safe transfer of keys across far larger networks.

This involves fine tuning key management protocols and authentication to address issues such as increasing response time while at the same developing a security model that is more robust for the users. Furthermore, it will also discuss the integration of the aforementioned quantum cryptography techniques with more modern forms of computing like edge computing and Internet of Things (IoT) to provide the overall security to the users in the complex and society distributed environment. There is also another significant direction for future research that entails intensive practical experiments with using these solutions in various clouds with the help of pilots. In the long run, the objective is to develop reference protocols of quantum cryptography that can be widely implemented to form a strong security layer against the third-generation threats.

References

[1] [1] M. C. V. and N. A. N., "A Hybrid Double Encryption Approach for Enhanced Cloud Data Security in Post-Quantum Cryptography. | International Journal of Advanced Computer Science &amp; Applications | EBSCOhost." Accessed: Aug. 21, 2024. [Online]. Available: https://openurl.ebsco.com/contentitem/doi:10.14569%2Fijacsa.2023.0141225?sid=ebsco:plink:crawler&id=ebsco:doi:10.14569%2Fijacsa.2023.0141225

[2] "A novel integrated quantum-resistant cryptography for secure scientific data exchange in ad hoc networks - ScienceDirect." Accessed: Aug. 21, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S157087052400218X

[3] "Strengthening security in cryptographic protocols in the era of quantum computers." Accessed: Aug. 21, 2024. [Online]. Available: https://journals.uob.edu.bh/handle/123456789/5588

[4] "Strengthening Implementation Security for Quantum Cryptography in the Era of Quantum Computing by Bridging Theory and Practice | IEEE Conference Publication | IEEE Xplore." Accessed: Aug. 21, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10568640

[5] "Adaptive Multi-Layered Cloud Security Framework Leveraging Artificial Intelligence, Quantum-Resistant Cryptography, and Systems for Robust Protection in Optical and Healthcare | Research Square." Accessed: Aug. 21, 2024. [Online]. Available: https://www.researchsquare.com/article/rs-3408257/v1

[6] R. Azhari and A. N. Salsabila, "Analyzing the Impact of Quantum Computing on Current Encryption Techniques," IAIC Transactions on Sustainable Digital Innovation (ITSDI), vol. 5, no. 2, Art. no. 2, Feb. 2024, doi: 10.34306/itsdi.v5i2.662.

[7] "Blockchain-based cyber-security trust model with multi-risk protection scheme for secure data transmission in cloud computing | Cluster Computing." Accessed: Aug. 21, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s10586-024-04481-9

[8] "Cryptography: Advances in Secure Communication and Data Protection | E3S Web of Conferences." Accessed: Aug. 21, 2024. [Online]. Available: https://www.e3s-conferences.org/articles/e3sconf/abs/2023/36/e3sconf_iconnect2023_07010/e3sconf_iconnect2023_07010.html

[9] "Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing | The Journal of Supercomputing." Accessed: Aug. 21, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s11227-023-05616-2

[10] "Securing IoT devices: A novel approach using blockchain and quantum cryptography - ScienceDirect." Accessed: Aug. 21, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660523003426

[11] "Cybersecurity Issues and Challenges in Quantum Computing - Topics in Artificial Intelligence Applied to Industry 4.0 - Wiley Online Library." Accessed: Aug. 21, 2024. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781394216147.ch11

[12] "Evaluating the Synergies Between Cloud Computing, Big Data Analytics, and Quantum Algorithms: Opportunities and Challenges | Journal of Empirical Social Science Studies." Accessed: Aug. 21, 2024. [Online]. Available: https://publications.dlpress.org/index.php/jesss/article/view/88

[13] "SAFEGUARDING DIGITAL SECURITY: ADDRESSING QUANTUM COMPUTING THREATS | The Role of Exact Sciences in the Era of Modern Development." Accessed: Aug. 21, 2024. [Online]. Available: https://uzresearchers.com/index.php/RESMD/article/view/873

[14] "Revolutionizing Cloud Security: Leveraging Quantum Computing and Key Distribution for Enhanced Protection | The Review of Socionetwork Strategies." Accessed: Aug. 21, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s12626-023-00140-4

[15] 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, Art. no. 1, Jun. 2024, doi: 10.52700/scir.v6i1.149.

[16] "Fuzzy-enhanced adaptive multi-layered cloud security framework leveraging artificial intelligence, quantum-resistant cryptography, and fuzzy systems for robust protection - IOS Press." Accessed: Aug. 21, 2024. [Online]. Available: https://content.iospress.com/articles/journal-of-intelligent-and-fuzzy-systems/ifs233462

[17] "Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography - ScienceDirect." Accessed: Aug. 21, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0140366421002036

[18] S. Singh and D. Kumar, "Enhancing Cyber Security Using Quantum Computing and Artificial Intelligence: A Review," International Journal of Advanced Research in Science Communication and Technology, vol. 4, pp. 2581–9429, Jun. 2024, doi: 10.48175/IJARSCT-18902.

[19] S. Agrawal, "Harnessing Quantum Cryptography and Artificial Intelligence for Next -Gen Payment Security: A Comprehensive Analysis of Threats and Countermeasures in Distributed Ledger Environments," Mar. 2024, doi: 10.21275/SR24309103650.

[20] H. Kadry, A. Farouk, E. A. Zanaty, and O. Reyad, "Intrusion detection model using optimized quantum neural network and elliptical curve cryptography for data security," Alexandria Engineering Journal, vol. 71, pp. 491–500, May 2023, doi: 10.1016/j.aej.2023.03.072.

[21] S. Dhar, A. Khare, A. D. Dwivedi, and R. Singh, "Securing IoT devices: A novel approach using blockchain and quantum cryptography," Internet of Things, vol. 25, p. 101019, Apr. 2024, doi: 10.1016/j.iot.2023.101019.

[22] D. Swetha and S. K. Mohiddin, "Quantum-Enhanced Security Advances for Cloud Computing Environments. | International Journal of Advanced Computer Science &amp; Applications | EBSCOhost." Accessed: Aug. 21, 2024. [Online]. Available: https://openurl.ebsco.com/contentitem/doi:10.14569%2Fijacsa.2024.01506118?sid=ebsco:plink:crawler&id=ebsco:doi:10.14569%2Fijacsa.2024.01506118

[23] 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, Jan. 2022, doi: 10.1016/j.matpr.2021.05.593.

[24] A. Aydeger, E. Zeydan, A. Yadav, K. Hemachandra, and M. Liyanage, Towards a Quantum-Resilient Future: Strategies for Transitioning to Post-Quantum Cryptography. 2024.

[25] "TSP_CMC_43439.pdf." Accessed: Aug. 21, 2024. [Online]. Available: https://cdn.techscience.cn/files/cmc/2024/TSP_CMC-78-1/TSP_CMC_43439/TSP_CMC_43439.pdf

[26] M. Azeez et al., "Quantum AI for cybersecurity in financial supply chains: Enhancing cryptography using random security generators," World Journal of Advanced Research and Reviews, vol. 23, no. 1, Art. no. 1, 2024, doi: 10.30574/wjarr.2024.23.1.2242.

[27] D. Dhinakaran, D. Selvaraj, N. Dharini, S. E. Raja, and C. S. L. Priya, "Towards a Novel Privacy-Preserving Distributed Multiparty Data Outsourcing Scheme for Cloud Computing with Quantum Key Distribution," arXiv.org. Accessed: Aug. 21, 2024. [Online]. Available: https://arxiv.org/abs/2407.18923v1

[28] U. Mmaduekwe and E. Mmaduekwe, "Cybersecurity and Cryptography: The New Era of Quantum Computing," Current Journal of Applied Science and Technology, vol. 43, no. 5, Art. no. 5, Apr. 2024, doi: 10.9734/cjast/2024/v43i54377.

[29] H. C. Ukwuoma, G. Arome, A. Thompson, and B. K. Alese, "Post-quantum cryptography-driven security framework for cloud computing,"

Open Computer Science, vol. 12, no. 1, pp. 142–153, Jan. 2022, doi: 10.1515/comp-2022-0235.

[30] S. Kanungo and S. Sarangi, "Quantum computing integration with multi-cloud architectures: enhancing computational efficiency and security in advanced cloud environments," World Journal of Advanced Engineering Technology and Sciences, vol. 12, no. 2, pp. 564–574, 2024, doi: 10.30574/wjaets.2024.12.2.0319.

[31] "Cloud workload." Accessed: Apr. 16, 2024. [Online]. Available: https://www.kaggle.com/datasets/akhilbs/cloud-workload

[32] D. Dhinakaran, D. Selvaraj, N. Dharini, S. E. Raja, and C. Priya, "Towards a novel privacy-preserving distributed multiparty data outsourcing scheme for cloud computing with quantum key distribution," arXiv preprint arXiv:2407.18923, 2024.

[33] S. Dhar, A. Khare, A. D. Dwivedi, and R. Singh, "Securing IoT devices: A novel approach using blockchain and quantum cryptography," Internet of Things, vol. 25, p. 101019, Apr. 2024, doi: 10.1016/j.iot.2023.101019.