A Revolutionary Approach Using Artificial Intelligence and Quantum Cryptography – A Review

Najma Imtiaz Ali [1], Imtiaz Ali Brohi [2], Mujeeb-ur-Rehman Jamali [2], Mazhar Basheer Arain [2] Abdul Rehman Nangraj [3]

[1] Faculty of Information and Communication Technology, University of Technology Malaysia Melaka, Malaysia

[2] Department of Computer Science, Government College University, Hyderabad, Sindh, Pakistan

[3] Institute of Mathematics and Computer Science, University of Sindh, Jamshoro, Pakistan

*__Correspondence__: imtiaz.brohi@gcuh.edu.pk

Citation | Ali. N. I., Brohi. I. A., Jamali. M. U. R. Arain. M. B, "A revolutionary approach using Artificial Intelligence and Quantum Cryptography – A Review", IJIST, Vol. 07, Issue. 03 pp 1422-1436, July 2025

DOI| https://doi.org/10.33411/ijist/20257314221436

Received| June 10, 2025 **Revised|** July 02, 2025 **Accepted|** July 07, 2025 **Published|** July 13, 2025.

Data security is one of the most important aspects of the digital world as technology evolves and expands. Existing cryptographic systems are vulnerable due to quantum threats. The integration of Artificial Intelligence with Quantum Cryptography is an emerging field. AI-driven methods in QC to mitigate and be robust against the quantum threat. Quantum computing uses quantum mechanics to process data very quickly and accurately. Quantum Machine Learning can process big data as compare to classical methods with much more efficiency. The synergistic combination improves the threat detection and classification with accuracy. The integration also significantly enhances the speed and scalability of the large-scale deployment. AI enhances the efficiency and security of QC systems, and the challenges and opportunities of using AI-powered integration of quantum computing are reviewed.

Keywords: Quantum Computing, Quantum Cryptography, Post-Quantum Cryptography, Artificial Intelligence, Quantum Machine Learning

Introduction:

In the digital era, data security has become a critical concern with the continuous advancement of technology. The emergence of Artificial Intelligence (AI) has enhanced the usability, practicality, and scalability of quantum computing (QC). The synergic relationship is immune to the various attacks using state-of-the-art technology. AI strengths are used for the detection of threats with a comprehensive strategy, with QC drastically. The paradigm has been shifted with the advent of quantum computing to ensure the security while data at motion. Quantum computing (QC), leveraging the principles of quantum mechanics, offers a promising approach to ensuring secure communication. The Modern Cryptographic (MC) systems are facing significant threats due to the rapid advancement of quantum computing. The development of systems that are secure against quantum attacks is known as quantum-resistant. These algorithms cannot be broken efficiently by quantum computers. As traditional cryptography uses mathematical hardness for secure communication and Post Quantum Cryptography (PQC) secures the communication in the advancement of quantum computing capabilities.

AI aids in the automatic identification of threats and facilitates timely responses. Moreover, AI and ML techniques have revolutionized various domains, including quantum communication [1]. ML is subbing subfield of AI; the model of ML can be used continuously to provide massive datasets security, detect flaws and anomalies. ML models can be continuously trained to secure large datasets, detect vulnerabilities, and identify anomalies. It has had a significant impact on quantum communication (QC), where its techniques are employed to analyze, enhance, and strengthen QC systems against potential threats such as quantum cryptanalysis. The speed of the key generation can be increased using Quantum Machine Learning (QML). The ML approach helps with fault-tolerant quantum computing and quantum error correction. It is also helpful to achieve reliable and secure communication, as well as to monitor anomalies. QML to handle huge datasets and automatically detect anomalies. To regulate the quantum entanglement using ML techniques [2]. QML supports Quantum Support Vector Machine (SVM) to process huge datasets much more efficiently. However, QML faces several challenges, including hardware limitations, the need for advanced algorithm development, error correction issues, and difficulties in integration with classical computing systems. There is a need for continued research to overcome these challenges. Synthesizing current and future studies is essential for identifying the full potential of QML.

Figure 1 illustrates cryptography and its subdomains, including modern cryptography (MC), quantum computing (QC), and post-quantum cryptography (PQC). The integration of Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), and Neural Networks (NNs) is also depicted and will be discussed in the following section.

Traditional security frameworks such as RSA, ECC, and classical symmetric encryption are fundamentally based on computational hardness assumptions (e.g., factorization, discrete logarithms) [3]. However, these assumptions are rendered vulnerable by quantum algorithms like Shor's and Grover's, which can break RSA and significantly reduce the strength of symmetric algorithms, respectively. This emerging threat landscape has accelerated the shift toward post-quantum cryptographic solutions, such as Quantum Key Distribution (QKD).

AI plays a dual role that is enhancing adaptive security systems that anticipate quantum attacks, and optimizing quantum cryptographic protocols and their implementations. This review explores and comprehensive analysis of the efficiency and security of QC systems. The opportunities and challenges in the convergence of AI and QC for secure are identified. It also provides the challenges faced by the MC due to the integration of AI. The review focuses on the conceptual understanding, analysis, and interpretation of existing literature. It is also

examined how ML-enhanced QC can be used in real-world settings such as secure communication, quantum networks, and other areas where quantum security is essential. The synthesizing finding, the current state of knowledge, and suggestions for future research direction. This integration is essential for developing secure systems in the post-quantum era.

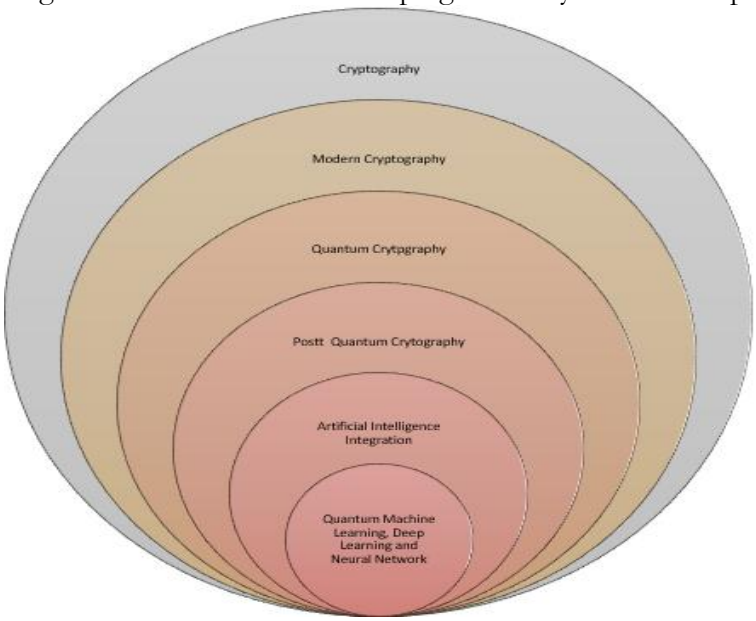

Figure 1. AI Integration to Quantum Cryptography

Modern Cryptography:

MCs are used to secure the data using cryptographic algorithms. The categories of cryptographic algorithms include symmetric algorithms such as DES, 3DES, AES, and Blowfish, and asymmetric algorithms such as DSA, RSA, ECC, and ElGamal. The security level of a symmetric algorithm is the secret key size, which provides a level of security. There are other factors, including the number of rounds, block size, and mode of encryption and decryption. The asymmetric algorithm relies on mathematical problems, including discrete logarithms, integer factorization, and mathematical equations. The size of the key pair (e.g., public and private key) provides a level of security, but there is time complexity for key generation and encryption, decryption and digital signature, and digital certificate generation and verification [4].

Quantum Computing:

Traditional computers work based on 0 or 1 bits. Quantum computing is in an infant and experimental stage; it uses simultaneously multiple states of quantum qubits; this principle of quantum mechanics enables to manipulation and performance of certain operations very quickly. Mathematical problems can be solved by quantum computers efficiently, which is computationally infeasible by traditional computers.

Quantum computing programs are written in Java and the Python programming language. There are standard libraries as well as a simulator for the development of problems. It represents a specified number of qubits that can simulate quantum circuits. Quantum Hadamard gate that puts a qubit into a superposition state. The execution environment shows the output that is the probabilities of the qubit in the $|0\rangle$ and $|1\rangle$ states. Quantum computers are designed to solve specific types of problems that involve simulating quantum systems.

Principles of Quantum Mechanics:

Quantum mechanics, a fundamental theory in physics, describes the behavior of energy and matter at the smallest scales, such as atoms and subatomic particles. The superposition is the ability that several states are at once. In quantum mechanics, entanglement is when particles are linked together; a particle has influence immediately to the other.

Quantum Key Distribution (QKD) algorithm makes it possible to obsolete the traditional encryption methods by quantum computers. It provides an alert for intrusions to parties, and it ensures every attempt to eavesdrop alters the quantum state [2]. It is the capability of quantum physics that allows for safe key exchange in QKD. There is a risk of a side-channel attack, which is mitigated by the QKD system. Using quantum computing to develop cryptanalysis methods poses a serious risk to the security of the system. Encrypted private data is vulnerable to potential threats posed by quantum computers, which may eventually have the capability to break current cryptographic algorithms. The growing power of quantum computing presents a significant future risk to data security.

The integrity of data is checked and verified by a digital signature. Quantum computing has the potential to break digital signatures. The authentication of the user and system is checked by using a digital certificate; a public key infrastructure system is used to prove the identity of the user and system. The overall security of the user and system is to be compromised by quantum computing.

Quantum computers can process vast amounts of data. Traditional systems are inadequate to process high-dimensional data. Smallest quantum computers are designed that are powered by a single photon; they can solve the complex problem of prime factorization, which is used in MC algorithms for key pair generation for confidentiality, integrity, and authentication in cryptographic systems. This is a breakthrough; it provides a major role for security and advancement in the quantum era. Figure 2 illustrates the threat detection process in quantum computers. Raw data is collected and processed in parallel using the principles of quantum mechanics, specifically the superposition of qubits. Quantum computers leverage quantum-enhanced algorithms, enabling them to handle complex and large datasets efficiently. As a result, they offer faster and more accurate threat detection capabilities.

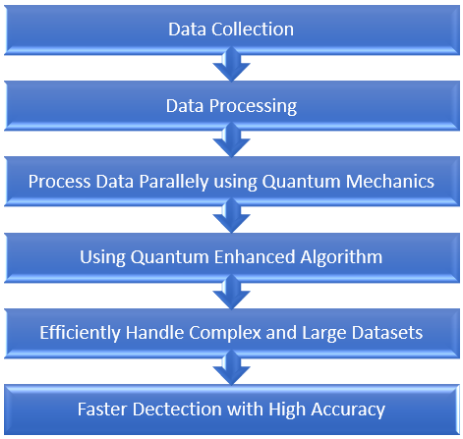

Figure 2. Quantum Threat Detection

In classical computers, collected data are processed sequentially, using deterministic algorithms, and these systems have limited scalability for complex and large datasets. These are slower for detection and have higher false positives for threat detection.

Authors stated that the advantage of quantum mechanics is that it to detect and correct an early stage through quantum error correction [5]. The implementation of post-quantum cryptography algorithms is essential because of the significant danger posed by quantum computing to conventional encryption techniques.

Quantum Cryptography:

The importance of QC has become increasingly important due to the arrival of quantum computers. QC is a branch of cryptography; it uses the principles of quantum mechanics to secure communication [6]. Modern cybersecurity systems can be broken in a short amount of time. Integration of QC with AI is very much important to address to pressing issue [2].

PQC and QC are two promising approaches to securing data in the quantum era. PQC algorithms are specifically designed to withstand and resist attacks from quantum computers. There is vulnerability for traditional systems due to the advent of quantum computing. The principles of quantum mechanics theoretically provide computationally infeasible and unbreakable security. The MC algorithm relies on mathematical problems that can be solved by a quantum computer.

The field of QC is rapidly changing with the advent of AI; it provides automatic enhancement in security, resultant robustness of the cryptographic algorithm, as well as defense in the digital world. The benefits of the AI integration in the field of QC to improving the key generation as well as anomaly detection. There are significant practical challenges, such as adversarial vulnerability and network optimization. AI-driven security frameworks are for QML and QKD. QKD uses quantum mechanics to secure the communication and mitigate the security issues of eavesdropping to intercept while securely distributing encryption and decryption keys. It is a prominent method that provides unbreakable encryption in QC.

Post-Quantum Cryptography:

QC has the potential to break the symmetric and asymmetric algorithms. It can quickly process the specific calculations which is computationally infeasible. Symmetric algorithm with a long size of secret key provides a level of security and is quantum-resistant. Asymmetric algorithms are at a higher risk of quantum attacks. These algorithms are commonly used for key exchange, digital signatures, and the generation and verification of digital certificates. Grover's and Shor's quantum algorithms can break the symmetric and asymmetric algorithms, respectively. Grover's algorithm, with quadratic complexity, can be used to accelerate the search in unstructured databases, thereby reducing the security level of symmetric encryption algorithms by effectively halving their key strength. On the other hand, Shor's algorithm, which operates with exponential efficiency, can factor large integers and compute discrete logarithms, making it capable of breaking widely used asymmetric algorithms such as RSA and ECC. It has a quantum primitive amplitude amplification while Shor's algorithm Quantum Fourier Transform. Grover's algorithm reduces symmetric key security while breaking Asymmetric Encryption, Key Exchange, and Digital Signature, i.e., RSA (3072 bit), DH (3072 bit), ECDH & ECDSA (256 bit) by Quantum algorithms respectively.

The emerging field of PQC is to mitigate the threat to current cryptosystems. To protect against and resist the QC attack, the PQC algorithms are designed. PQC is built on mathematical problems that are considered hard and secure against quantum attacks. Figure 3 shows the PQC algorithms, including code, lattice- and hash-based cryptography. PQC algorithms also include isogeny-based cryptography and multivariate polynomials.

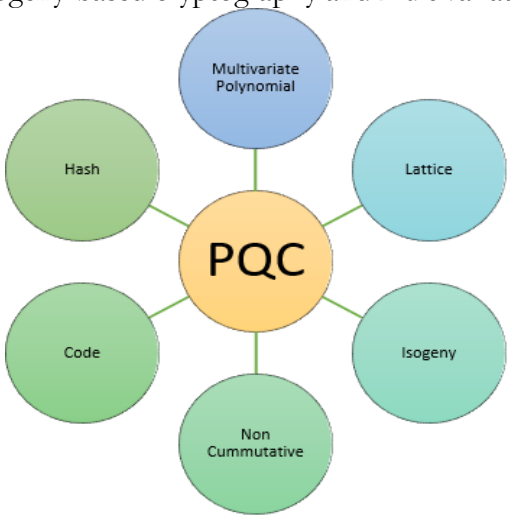

Figure 3. Post Quantum Cryptography

There is growing interest in PQC algorithms for immune mitigation from quantum attacks. PQC algorithms are mathematically robust against quantum attacks. PQC is also feasible in existing hardware and infrastructures. There are challenges of standardization and computational overhead to PQC.

Artificial Intelligence:

According to the father of AI, John McCarthy, it is "The science and engineering of making intelligent machines, especially intelligent computer programs". AI is a field of science and technology focused on developing computer programs capable of reasoning, learning, and problem-solving, abilities typically associated with human intelligence. ML is sub sub-branch of AI. Similarly, DL is sub sub-subfield of ML. Figure No.4 shows the QAI interface.

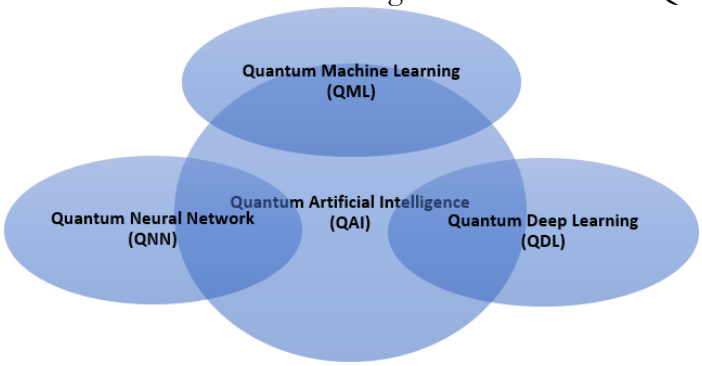

Figure 4. Quantum Artificial Intelligence

Machine Learning:

ML provides the ability without explicitly programmed computer can learn and grow with change when exposed to new data. It also provides the ability to analyze large, complex datasets automatically, which is a demand of modern applications. Data-driven tasks, statistical analysis, and decision-making can be done automatically with reasoning. Its application is almost in every area, such as cybersecurity, health, natural language and image processing, scientific imaging, and neuroscience. Some broad areas of ML are classification, regression, ranking, clustering, and dimensionality reduction. ML models are vulnerable due to adversarial attacks, that is, intentional manipulation of input data to make incorrect predictions. Adversarial attacks are due to weaknesses of ML systems and can impact various applications. Figure 5 shows the types of ML algorithms.

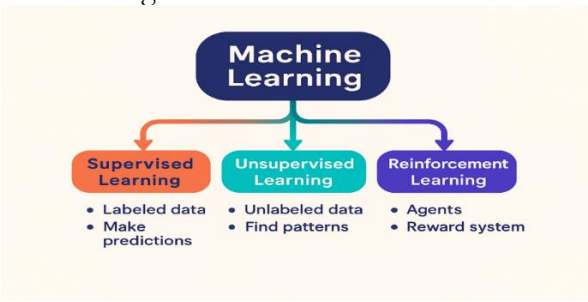

Figure 5. Machine Learning types of algorithms

Supervised Learning (SL):

SL algorithms use labelled data to learn. The datasets use the output label to train the data. Input data (feature) belongs to the targeted variable output label. The prediction task classifies based on the learned patterns to predict new and unseen data. Some of the most well-known Machine Learning algorithms include Logistic Regression, Naive Bayes, and Support Vector Machines (SVMs), among others.

Unsupervised Learning (USL):

Unsupervised Learning (USL) algorithms use unlabeled data to identify patterns and structures within the dataset. In this approach, the input data does not have explicitly labeled

outputs, and the model learns without direct supervision. The prediction task identifies patterns in the data without any predefined label. USL performs clustering same type of data point and dimensionality reduction of the data. Some of the most well-known Unsupervised Learning algorithms include Principal Component Analysis (PCA), K-Means Clustering, and Hierarchical Clustering.

Reinforcement Learning (RL):

In the RL, an agent interacts and learn based on rewards and penalties for its actions. Reinforcement Learning involves taking new actions through exploration while also utilizing known successful actions through exploitation. Striking a balance between these two is crucial for optimal learning. Well-known algorithms in this field include Q-Learning, Policy Gradient methods, and Deep Q-Networks (DQN). The following table 1 shows the complexity of the various types of ML algorithms, e.g., supervised, unsupervised, reinforcement, regression, classification, classification/regression, clustering, dimensionality reduction, and decision making. While ML helps reduce problem complexity and improve efficiency, Genetic Algorithms are particularly effective when it comes to optimization tasks.

Table 1. Comparison of ML Algorithms with complexity

1.	Linear Regression	2.0
2.	Logistic Regression	2.0
3.	Decision Tree	3.0
4.	Random Forest	4.0
5.	SVM	4.0
6.	Neural Network	3.0
7.	K-Means	3.0
8.	Hierarchical Clustering	4.0
9.	Q-Learning	4.0

Machine Learning Algorithms for Quantum Cryptographic Applications:

QML is an emerging field that provides a transformative approach to secure data in motion with quantum mechanics. It has the potential to resist eavesdropping, and it provides a level of security compared to traditional cryptographic algorithms. The field of quantum evolves, there are limitations and practical applications, but theoretically, it provides information security. The following figure 6 shows that the quantum enhancement process involves data acquisition and preprocessing, along with cleaning work, feature extraction with a quantum optimization algorithm thereafter threat detection is done using the QML algorithm, which is QSVM.

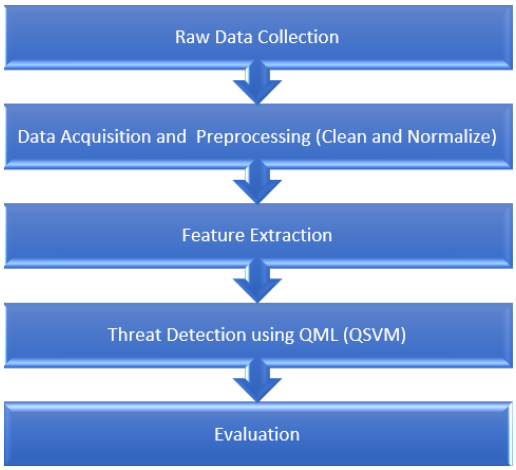

Figure 6. Quantum Enhancement

ML has significantly impacted various fields, including QC. ML contributes to strengthening QC systems by detecting threats, optimizing encryption processes, and

improving overall efficiency. It also provides automatic decision-making. ML-driven security to ensure secure communication. QC algorithms use ML techniques to exploit the weaknesses in quantum analysis. Cryptanalysis employs the performance of quantum mechanics, which is optimized with the use of ML. Patterns are identified, and anomalies in training an ML model on big datasets.

Intrusion detection in Quantum Communication can be performed using Support Vector Machines (SVMs). SVMs are effective in classifying anomalies and identifying potential security breaches within quantum communication systems. Reinforcement Learning (RL) can be used to adjust quantum parameters, optimizing the process of secure key generation. In quantum cryptographic systems, RL aids in threat detection and response by enabling the system to automatically learn from attacks and continuously improve its defensive strategies. In quantum communication, anomalies are detected using Decision Trees (DT). DT and Random Forest (RF) are used, respectively, for intrusion detection in QC. RF is used in quantum cryptographic techniques to secure and optimize datasets. Analyzing the large datasets and optimization can be done using RF. Quantum different states can be classified using K-Mean Clustering for secure key exchange and anomaly detection. The eavesdropping can be identified and detected by unusual patterns in the quantum communication. Quantum Noise Reduction is done using the Generative Adversarial Network (GANs) in the QC. Artificial datasets can be generated and processed for training by GANs. It also simulates quantum attacks; it helps to develop robust encryption algorithms. NNs can significantly enhance security parameters by using dynamic error detection. In the Quantum communication process, error detection can be done by Deep Neural networks (DNNs), which enhance the efficiency of the QKD.

In traditional cryptographic systems, algorithms are challenges and vulnerability due to quantum computing. There are opportunities to integrate ML with quantum-resistant cryptographic systems, key generation, threat detection, and enhancing protocol optimization. Dynamic adaptation and hybrid models are suggested. It also has potential risks due to adversarial vulnerabilities. This approach creates a robust and scalable cryptographic system for secure communication. Existing algorithms are susceptible to quantum attack; there is a requirement to create quantum-resistant cryptography to mitigate these vulnerabilities.

Literature Review:

ML is a branch of AI that enables systems to make predictions based on data without being explicitly programmed. The integration of ML can significantly enhance the capabilities of QC. It provides security, efficiency, and usability. The model is created in ML to recognize patterns based on model data and predictions. There are various areas where applications are such as computer vision, NLP, and predictive analytics, using techniques of ML. In ML models, data may be manipulated, thus incorrect predictions or unintended outcomes may occur due to Adversarial attacks. The vulnerabilities of the models may cause the model may misclassify or fail to predict data correctly.

According to the authors, using GANs to improve training by generating artificial datasets for noise detection in quantum systems. It helps to develop strong encryption algorithms. GANs can be used in quantum networks for cryptographic resilience and to simulate adversarial attacks [7].

Quantum computing has made its mark in finding aberrant events in vast quantities of information. Anomalies of all sorts can be found quickly as large quantities are tested simultaneously. Quantum-enhanced anomaly detection algorithms can accelerate the identification of rare events and patterns, offering faster and more efficient threat detection. For example, Quantum Principal Component Analysis (QPCA), a technique developed for quantum machine learning, can be used to reduce the dimensionality of datasets and facilitate clustering. This type of analysis also offers insights into what may constitute an anomaly [8].

As noted in [9], the application of ML in Quantum Computing offers numerous opportunities across various fields, but it also presents several challenges. The author of this study reviewed state-of-the-art approaches in quantum computation with the integration of AI and ML models. ML models can be employed for quantum error correction, quantum computing, and quantum communication. They are also used to efficiently map quantum algorithms onto existing quantum hardware. Authors [10] stated that traditional cryptographic algorithms face unprecedented challenges from quantum computing. Symmetric and asymmetric algorithms are vulnerable to quantum attacks. There is also the advent of quantum-resistant cryptography as an important field that employs lattice, hash-based algorithms to counter quantum threats. Authors [11] stated that quantum random number is generated using quantum mechanics for cryptographic security. This significantly enhances the security of the cryptographic systems. In [10] authors stated that there are new security risks due to the integration of ML in quantum cryptography. The model's weakness can be exploited by the adversarial attacks.

QC uses the principles and mechanics to secure communication by QKD. ML integration provides error correction and protocol efficiency; it is vulnerable to adversarial attacks. QML processes the quantum data more efficiently, but it faces model trainability challenges.

Quantum computing can advance the area where it is applied; there are also challenges for existing contemporary computing [10]. Shor's algorithm can solve the effective problem of factoring large prime numbers. This is also a serious risk for existing cryptographic systems that depend on an asymmetric algorithm pair of key generation for encryption and decryption, as well as digital signature generation and verification.

QC's Grover's algorithm has the potential to search an unsorted database quickly. It does shorten the key length needed in the brute force attack. The victims of this attack are symmetric algorithms and hash functions, which can be broken quickly through cryptanalysis. The impact of Grover's algorithm is less severe on asymmetric algorithms. The encrypted data is nonetheless at risk when quantum machines are used by adversaries to access and decrypt it.

ML in QC represents a cutting-edge fusion of AI and quantum technologies. It enhances the security and effectiveness of quantum communication systems. ML methods are used to enhance the key generation, error correction, and quantum state estimation, and it is also used in QKD. ML techniques are used in cryptanalysis analytics to suggest a particular QKD algorithm for the case. It also enhances the quantum random key generation. QC integration with ML has the potential to secure the communication paradigms.

QC uses principles of quantum mechanics; ML algorithms can be used for the enhancement of data in motion. There are opportunities as well as potential risks that need to be considered. Researchers, policymakers need to carefully consider challenges in this interdisciplinary field [10].

Authors [12] stated that traditional cryptosystems are broken by quantum computers. Symmetric algorithms AES, 3DES, etc., are vulnerable to Grover's algorithm key search process is reduced square root of the original time. The asymmetric algorithms RSA and ECC are vulnerable to Shor's algorithm, which solves mathematical problems in polynomial time to break the keys that are used for confidentiality, integrity, and authentication [13].

A cryptographic algorithm is used to secure the transaction and data in the Blockchain. The integrity of a block in the Blockchain is validated by an asymmetric algorithm. The security of the Block may be compromised by quantum computing.

Cybersecurity can be significantly improved through Quantum Computing's ability to solve complex optimization problems [14]. The emergence of quantum computing has had a profound impact on the field of cybersecurity, particularly due to its potential to break widely used asymmetric cryptographic algorithms. The security of these algorithms—such as RSA

and ECC is based on the computational hardness of mathematical problems like integer factorization and discrete logarithms. A large factor can be generated by a quantum computer efficiently using Shor's algorithm, which substantial risk to the security of the existing system that uses these algorithms for encryption [15].

For security enhancement, NN based on the environment factor can adjust QKD dynamically [10]. QNN and DL models face model trainability challenges. Optimization of QKD and securing secret key, as well as communication error reduction, NN can be applied [10]. In this research [16][11][17][18], according to the authors, QKD theoretically is secure, and it provides a level of security based on quantum mechanics. Secure key information is communicated using qubits. The secret key is used in a symmetric algorithm for transforming data into an unreadable format, and it provides data confidentiality and privacy while in transmission and protects from eavesdropping [19][20][21]. Quantum channels require qubits consisting of information about a secret key that is shared over the public domain; the communication is done through a quantum channel [1].

In [22][23][24][25], authors stated that with the advent of AI, advanced problems can be solved using a model to predict using a particular AI algorithm. AI systems are used to statistically analyze large datasets and recognize patterns and make decisions or predictions based on data [26]. ML is a branch of AI in which algorithms are designed to learn from data and make predictions without being explicitly programmed [27]. Authors [28] stated that ML systems can be used to process big datasets, and predictions can be made based on data. There are a number of domains where unprecedented opportunities including quantum communications [29][30][31][32].

ML algorithms are classified according to the input dataset process and prediction, that is, supervised, unsupervised, and reinforcement learning [33]. Supervised learning uses labeled data, but unsupervised learning makes predictions on data based on unlabeled data [25]. Moreover, Reinforcement learning is inspired by behavioral and neuroscience [34]. RL is an agent-specific form, and it is based on reward and penalty to its environment via perception and action. DL is a subset of ML; it has processing units to learn multiple levels of abstraction, and it is composed of multiple layers of given data to process. Most significantly, DL is used in many domains, and it is basic in high-dimensional data to discover structures [35][36].

According to authors that ML can significantly improve PQC algorithms for quantum-resistant hash and lattice algorithms [10]. In [37] authors found that vulnerabilities of the PQC algorithms from quantum threats can be mitigated, and anomaly detection can be done. For optimal security, Machine Learning (ML) algorithms can automate the selection and classification of Post-Quantum Cryptography (PQC) algorithms [38]. PQC algorithms' vulnerabilities are detected and classified by using SVMs [38]. Additionally, Decision Trees (DT) can be employed to improve PQC security and automate key selection processes [7]. Overall, Machine Learning (ML) algorithms enhance PQC by reinforcing security measures and optimizing key management.

Quantum-based attacks can be prevented by developing PQC. PQC algorithms utilize various techniques specifically designed to resist the computational power of quantum computers [39]. Quantum-resistant ML algorithms can be used to identify vulnerabilities in the encryption process and to secure against adversarial attack [37]. Malicious activities are detected using AI in quantum communication networks. Anomaly detection is ensured in Quantum Cryptographic security [7]. Side Channel attacks are detected by ML models. AI integrated with quantum to significantly improve intrusion detection with accuracy. RL is used to improve QKD network, it improves encryption rate and also reduces computational overhead [37]. Data patterns are analyzed for security enhancement using K-Means clustering [38]. Quantum keys are managed and optimized by using AI-based algorithms, and they ensure

secure communication. PQC enhances cybersecurity and provides robust protection from quantum computing's potential threats [40].

Quantum mechanics enhances cybersecurity by advancing secure communication. QKD is quantum secure communication, and it provides maximum protection in the communication channels. It is used to exchange the secret key between parties. While communication secret key, any attempt to eavesdrop and intercept an alert alerts the parties to the presence of the intrusion. This innovative approach provides great protection of the sensitive data against unauthorized access and interception. It is important for cybersecurity to provide security while data is transmitted [41]. Existing reviews do not consider the implications of quantum attacks. We uniquely address AI's adaptation for quantum-resilient systems. Our review contrasts with a broader scope involving real-world deployments, challenges, and architecture models.

Material and Method:

In this research work, a rigorous and unbiased qualitative analysis of the existing work on MC, QC, and PQC is done. The challenges and opportunities of the cryptographic system are also analyzed. The key problems, including the enhancement of quantum cryptographic protocols through the integration of AI, the main challenges associated with combining QC and AI, and the emerging opportunities of the integration presented. The study also explores how this convergence can influence future research and applications.

Figure 7 shows the research design that follows the scoping and research formulation, identifying the relevant up-to-date work in the area of the study, excluding the irrelevant, then conducting thematic analysis and synthesizing the key concepts from the literature, synthesizing findings and discussion insights from the review.

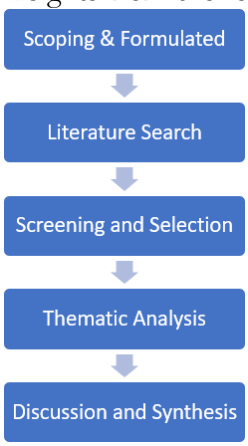

Figure 7. Flow Chart of Methodology

Foundational and cutting-edge studies, the timeframe was 2009–2025. The inclusion criteria were Peer-reviewed journals, conferences, and preprints with substantial contributions to AI, QC, or their integration. The relevant research was searched in the databases in the well-known sources, i.e., SpringerLink, IEEE Xplore, ACM Digital Library, and ScienceDirect. The keywords were used, i.e., "Artificial Intelligence", "Quantum Cryptography", "AI and Quantum Integration", "Cybersecurity", Post-Quantum Security", "Quantum Machine Learning", "AI-based Quantum Security".

Discussion:

The synergistic combination of AI and QC has various opportunities as well as challenges. The following are analyzed from a thorough literature review: AI has a significant role in cybersecurity due to ML algorithms to can quickly and accurately identify patterns, anomalies, and threat detection within big datasets. ML techniques are used in designing and optimizing various symmetric algorithms. AI-driven methods to create and enhance the efficiency of cryptographic algorithms, and it also analyzes nonlinearity and differential

uniformity properties of S-boxes (the most important component in symmetric algorithms. The problem's complexity is also reduced, and efficiency is improved.

NN has the potential to enhance the cryptographic system; it is employed for the deployment of cryptographic algorithms. In existing cryptographic algorithms, AI-driven methods are also used to automate the process of cryptanalysis. By NN training, learned models can predict the secret key to decrypt private and confidential data without the secret key due as AI fusion makes them vulnerable to existing cryptographic systems. Dynamic error detection is done using NN, which enhances the efficiency of the QKD in quantum communication. Quantum mechanics, such as superposition, allows quantum computers to simultaneously evaluate multiple possibilities using quantum entanglement, which correlates the properties of separated particles. Computational work is done efficiently and quickly compared to classical computers in a quantum computer. There is a need for integration of AI with quantum-resistant withstand the capabilities of quantum computers. The AI-driven optimization techniques can significantly enhance to creation secure and efficient PQC algorithm that ensures protection of privacy and confidentiality in the quantum era.

RL algorithms are used to learn from attacks and improve defenses. It is used in threat detection and response in a quantum cryptographic system. Intrusion detection in QC is done by using the DT and RF algorithms to secure and optimize datasets. K-Mean clustering is used to secure the sharing of the secret key and also to detect anomalies. Quantum communication eavesdropping is identified and detected using unusual patterns.

GANs are used to reduce quantum noise in the QC. For cryptographic security, the integration of AI with QC is feasible for advancement. AI algorithms make quantum cryptographic protocols more adaptable and efficient quantum cryptographic protocols. Mitigation of quantum threat, AI-driven approaches provide a pathway to optimize and develop quantum-resistant cryptographic algorithms. For the enhancement of data privacy, data at rest and data in motion, and robust security of the system, successful AI implementations have potential in enhancing quantum cryptographic systems, and also for the future.

There are challenges in integrating AI with a quantum cryptographic system. The integration process is complex, which depends on volume, quality of data, security and privacy, and potential biases. There are challenges in implementing AI-driven QC for real-time applications. There are also challenges of performance and scalability for the large-scale transformation of data and communication over the network. There is a challenge that requires significant resources and infrastructure for large-scale deployments.

Conclusion:

Data security can be enhanced using quantum computing and AI. PQC is considered a current cryptography practical solution, but secure communication in the future will require QC. Smallest quantum computers are designed that are powered by a single photon; they can solve the complex problem of prime factorization, which is used in MC algorithms for key pair generation for confidentiality, integrity, and authentication in cryptographic systems. This is a breakthrough; it provides a major role for security and advancement in the quantum era. There is a need hybrid approach and advancing standardization efforts. ML-driven security is very important in the quantum era to ensure secure communication. Security enhancement, key generation can be optimized, and anomaly detection can be detected using ML integration with the QC system. The hybrid approach ensures that in the quantum computing era, cryptographic protocols remain resilient. ML optimizes encryption algorithms, it also enhances QC, detects security threats, and automates predicting and decision making. ML algorithms can be used for the enhancement of data in motion. There are opportunities as well as potential risks that need to be considered. It is found that enhances and is strong against sophisticated attacks fusion of quantum cryptanalysis and ML. This synergy can lead to secure and provide

maximum data privacy efficiency in quantum communication using ML. QML quantum SVM can handle big datasets much more efficiently than classical methods, so it enables better threat detection. There are challenges due to the integration of AI into modern cryptography. ML enhances data privacy and security; QC has restrictions as well as difficulties. ML algorithms are significantly issue to adversarial attacks. Adversaries can take advantage of the weakness of ML models to gain access to quantum cryptographic confidential data. Further, ML algorithms have a need lot of training data, and there is an issue of private data use in models. There are attacks and security gaps with integrating ML and QC to assure the system's overall security. It is a crucial aspect that needs careful consideration in the development and deployment of such systems for the protection of data privacy and security. For a secure and resilient digital future in the quantum era, there is a need to foster collaboration between academia, policymakers, and the cryptographic community. Researchers, policymakers need to carefully consider challenges in this interdisciplinary field. This review provides insights for secure communication systems, cybersecurity, data privacy, and confidentiality in the future.

Authors' Contribution Statement:

This work was carried out in collaboration between all authors. Dr. Najma Imtiaz Ali: Conceptualization and Methodology. Prof. Dr. Imtiaz Ali Brohi: Reviewing & Editing. Dr. Mujeeb-ur-Rehman Jamali: Conducted research, Analysis, Interpretation and Written Original Draft of the Manuscript. Mr. Mazhar Basheer Arain: Literature Review and Referencing. Mr. Abdul Rehman Nangraj: Data Curation and Acquisition of data. All authors read and approved the final manuscript.

Conflict of interest: No.

References:

[1] M. Mafu, "Advances in artificial intelligence and machine learning for quantum communication applications," *IET Quantum Commun.*, vol. 5, no. 3, pp. 202–231, Sep. 2024, doi: 10.1049/QTC2.12094;WGROUP:STRING:PUBLICATION.

[2] A. H. Hussain, N. Hasan, N. U. Prince, M. Islam, S. Islam, and S. K. Hasan, "Enhancing cyber security using quantum computing and Artificial Intelligence: A review," *World J. Adv. Res. Rev.*, vol. 2021, no. 03, pp. 448–456, 2021, doi: 10.30574/wjarr.2021.10.3.0196.

[3] U. U. Mujeeb-ur-Rehman Jamali, Najma Imtiaz Ali, Imtiaz Ali Brohi, Muhammad Umar Murad, Yasir Nawaz, "An Empirical Evaluation of Data Integrity Algorithm Performance in Non-Relational Document Databases," *VAWKUM Trans. Comput. Sci.*, vol. 11, no. 2, pp. 70–82, 2023, doi: https://doi.org/10.21015/vtcs.v11i2.1663.

[4] A. Jamali, Mujeeb-ur-Rehman; Ali, Najma Imtiaz; Memon, Abdul Ghafoor; Maree, Mujeeb-u-Rehman; and Jamali, "Architectural Design for Data Security in Cloud-based Big Data Systems," *Baghdad Sci. J.*, vol. 21, no. 9, 2024, [Online]. Available: https://bsj.uobaghdad.edu.iq/home/vol21/iss9/5/

[5] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, vol. 52, no. 4, p. R2493, Oct. 1995, doi: 10.1103/PhysRevA.52.R2493.

[6] P. Radanliev, "Artificial intelligence and quantum cryptography," *J. Anal. Sci. Technol.*, vol. 15, no. 1, pp. 1–17, Dec. 2024, doi: 10.1186/S40543-024-00416-6/FIGURES/3.

[7] A. Jenefa, V. Ebenezer, A. J. Isaac, J. Marshell, P. Pradeepa, and V. Naveen, "Adversarial Attacks on Generative AI Anomaly Detection in the Quantum Era," *7th Int. Conf. Electron. Commun. Aerosp. Technol. ICECA 2023 - Proc.*, pp. 1833–1840, 2023, doi: 10.1109/ICECA58529.2023.10395092.

[8] E. Farhi, J. Goldstone, S. Gutmann, and H. Neven, "Quantum Algorithms for Fixed Qubit Architectures," Mar. 2017, Accessed: Jun. 17, 2025. [Online]. Available: https://arxiv.org/pdf/1703.06199

[9] D. Bhoumik, S. Sur-Kolay, L. K. K. J., and S. S. Iyengar, "Synergy of machine

learning with quantum computing and communication," Oct. 2023, Accessed: Jun. 17, 2025. [Online]. Available: https://arxiv.org/pdf/2310.03434

[10] P. A. Adepoju, B. Austin-Gabriel, A. B. Ige, N. Y. Hussain, O. O. Amoo, and A. I. Afolabi, "Machine learning innovations for enhancing quantum-resistant cryptographic protocols in secure communication," *Open Access Res. J. Multidiscip. Stud.*, vol. 4, no. 1, pp. 131–139, Sep. 2022, doi: 10.53022/OARJMS.2022.4.1.0075.

[11] R. Renner and R. Wolf, "Quantum Advantage in Cryptography," *AIAA J.*, vol. 61, no. 5, pp. 1895–1910, Jun. 2022, doi: 10.2514/1.J062267.

[12] D. J. Bernstein, "Introduction to post-quantum cryptography," *Post-Quantum Cryptogr.*, pp. 1–14, Jan. 2009, doi: 10.1007/978-3-540-88702-7_1.

[13] "Post-Quantum Cryptography | CSRC." Accessed: Jun. 17, 2025. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography

[14] A. Jadhav, A. Rasool, and M. Gyanchandani, "Quantum Machine Learning: Scope for real-world problems," *Procedia Comput. Sci.*, vol. 218, pp. 2612–2625, Jan. 2023, doi: 10.1016/J.PROCS.2023.01.235.

[15] Shoumya Singh and Deepak Kumar, "Enhancing Cyber Security Using Quantum Computing and Artificial Intelligence: A Review," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 4–11, Jun. 2024, doi: 10.48175/IJARSCT-18902.

[16] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, p. 145, Mar. 2002, doi: 10.1103/RevModPhys.74.145.

[17] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, no. P1, pp. 7–11, Dec. 2014, doi: 10.1016/J.TCS.2014.05.025.

[18] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, p. 661, Aug. 1991, doi: 10.1103/PhysRevLett.67.661.

[19] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, "The Security of Practical Quantum Key Distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Feb. 2008, doi: 10.1103/RevModPhys.81.1301.

[20] M. Mafu and M. Senekane, "Security of Quantum Key Distribution Protocols," *Adv. Technol. Quantum Key Distrib.*, May 2018, doi: 10.5772/INTECHOPEN.74234.

[21] K. Karabo, C. Sekga, C. Kissack, M. Mafu, and F. Petruccione, "A novel quantum key distribution resistant against large-pulse attacks," *IET Quantum Commun.*, vol. 5, no. 3, pp. 282–290, Sep. 2024, doi: 10.1049/QTC2.12089.

[22] "Artificial Intelligence for the Real World." Accessed: Jun. 17, 2025. [Online]. Available: https://hbr.org/webinar/2018/02/artificial-intelligence-for-the-real-world

[23] C. Janiesch, P. Zschech, and K. Heinrich, "Machine learning and deep learning," *Electron. Mark.*, vol. 31, no. 3, pp. 685–695, Apr. 2021, doi: 10.1007/s12525-021-00475-2.

[24] "Artificial Intelligence: A Modern Approach." Accessed: Jun. 17, 2025. [Online]. Available: https://www.pearson.com/en-us/subject-catalog/p/artificial-intelligence-a-modern-approach/P200000003500/9780137505135?srsltid=AfmBOoqb0YgCTklkTw235M61b3Yqugl95hJVcNJLb3R0pgY1e_SIT7fA

[25] "Pattern Recognition and Machine Learning | SpringerLink." Accessed: Jun. 17, 2025. [Online]. Available: https://link.springer.com/book/9780387310732

[26] P. Mehta *et al.*, "A high-bias, low-variance introduction to Machine Learning for physicists," *Phys. Rep.*, vol. 810, pp. 1–124, May 2019, doi: 10.1016/j.physrep.2019.03.001.

[27] "What Is Machine Learning (ML)? | IBM." Accessed: Jun. 17, 2025. [Online]. Available: https://www.ibm.com/think/topics/machine-learning

[28] B. M. Lake, T. D. Ullman, J. B. Tenenbaum, and S. J. Gershman, "Building Machines That Learn and Think Like People," *Behav. Brain Sci.*, vol. 40, Apr. 2016, doi: 10.1017/S0140525X16001837.

[29] Y. Lecun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015, doi: 10.1038/NATURE14539;SUBJMETA=117,639,705;KWRD=COMPUTER+SCIENCE,MATHEMATICS+AND+COMPUTING.

[30] M. Schuld and F. Petruccione, "Machine Learning with Quantum Computers," 2021, doi: 10.1007/978-3-030-83098-4.

[31] K. T. Schütt, S. Chmiela, O. A. von Lilienfeld, A. Tkatchenko, K. Tsuda, and K.-R. Müller, Eds., "Machine Learning Meets Quantum Physics," vol. 968, 2020, doi: 10.1007/978-3-030-40245-7.

[32] G. Carleo *et al.*, "Machine learning and the physical sciences," *Rev. Mod. Phys.*, vol. 91, no. 4, Mar. 2019, doi: 10.1103/RevModPhys.91.045002.

[33] C. Jiang, H. Zhang, Y. Ren, Z. Han, K. C. Chen, and L. Hanzo, "Machine Learning Paradigms for Next-Generation Wireless Networks," *IEEE Wirel. Commun.*, vol. 24, no. 2, pp. 98–105, Apr. 2017, doi: 10.1109/MWC.2016.1500356WC.

[34] K. Merrick and M. Lou Maher, "Motivated reinforcement learning: Curious characters for multiuser games," *Motiv. Reinf. Learn. Curious Characters Multiuser Games*, pp. 1–206, 2009, doi: 10.1007/978-3-540-89187-1/COVER.

[35] W. Ma, Z. Liu, Z. A. Kudyshev, A. Boltasseva, W. Cai, and Y. Liu, "Deep learning for the design of photonic structures," *Nat. Photonics 2020 152*, vol. 15, no. 2, pp. 77–90, Oct. 2020, doi: 10.1038/s41566-020-0685-y.

[36] M. Kraus, S. Feuerriegel, and A. Oztekin, "Deep learning in business analytics and operations research: Models, applications and managerial implications," *Eur. J. Oper. Res.*, vol. 281, no. 3, pp. 628–641, Mar. 2020, doi: 10.1016/J.EJOR.2019.09.018.

[37] V. Dhote, M. Sadim, P. Tanna, and A. N. Tiwari, "Machine Learning Strategies in Quantum-Resistant Network Security Protocols," *3rd IEEE Int. Conf. ICT Bus. Ind. Gov. ICTBIG 2023*, 2023, doi: 10.1109/ICTBIG59752.2023.10456284.

[38] B. S. Rocha, J. A. M. Xexeo, and R. H. Torres, "Post-quantum cryptographic algorithm identification using machine learning," *J. Inf. Secur. Cryptogr.*, vol. 9, no. 1, pp. 1–8, Dec. 2022, doi: 10.17648/JISC.V9I1.81.

[39] G. Yalamuri, P. Honnavalli, and S. Eswaran, "A Review of the Present Cryptographic Arsenal to Deal with Post-Quantum Threats," *Procedia Comput. Sci.*, vol. 215, pp. 834–845, Jan. 2022, doi: 10.1016/J.PROCS.2022.12.086.

[40] H. Gonaygunta, G. S. Nadella, P. P. Pawar, and D. Kumar, "Study on Empowering Cyber Security by Using Adaptive Machine Learning Methods," *2024 Syst. Inf. Eng. Des. Symp. SIEDS 2024*, pp. 166–171, 2024, doi: 10.1109/SIEDS61124.2024.10534694.

[41] N. Jain *et al.*, "Future proofing network encryption technology with continuous-variable quantum key distribution," Feb. 2024, Accessed: Jun. 17, 2025. [Online]. Available: https://arxiv.org/pdf/2402.18881