ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Advancing Secure Communication in the Quantum Era through the Integration of Artificial Intelligence and Quantum Cryptographic Techniques

Mr. Hemant N. Chaudhari

Assistant Professor, CSE [CyberSecurity], G H Raisoni College of Engineering and Management, Pune

DOI: https://doi.org/10.51583/IJLTEMAS.2026.150500034

Received: 03 May 2026; Accepted: 07 May 2026; Published: 26 May 2026

ABSTRACT

Utilizing the ideas of quantum physics, quantum cryptography is quickly becoming a vital defense against the growing cybersecurity risks of the contemporary day, especially in light of developing quantum computing. This essay investigates the complex field of quantum cryptography and looks at how it can transform network security and protect private data. We examine the fundamental ideas of quantum cryptography, such as Quantum Key Distribution (QKD) protocols like BB84 and E91, which use quantum features like superposition and entanglement to provide potentially indestructible secure communication channels. We also discuss the urgent need for quantum-resistant solutions in view of the developing "quantum threat" to well-known cryptographic algorithms like RSA and AES. The potential benefits and difficulties of using artificial intelligence (AI) techniques to boost quantum cryptography systems' resilience and efficiency are also examined. The creation of effective quantum repeater networks and enhanced security proofs are among the outstanding research topics, future difficulties, and present implementations in quantum cryptography that are covered in this study. We stress how crucial quantum cryptography is to protecting sensitive communications in the quantum era for a variety of industries, including the military, government, financial industry, and healthcare. We come to the conclusion that quantum cryptography has enormous potential for protecting vital information systems from future cyberattacks that are becoming more complex, even if we acknowledge the technology's early stages of development.

Index Terms – Quantum Computing, Quantum Cryptography, Quantum Key Distribution (QKD), Quantum Threat, Artificial Intelligence (AI), Secure Communication.

INTRODUCTION

In the field of cryptography, the advent of quantum computing offers both possibilities and problems. Existing cryptography methods are at risk from quantum computers, even though they have the ability to transform whole sectors by resolving difficult issues [1]. Researchers have responded by using quantum cryptography, which makes use of quantum physics to provide safe communication techniques that are impervious to both classical and quantum assaults. A important method for securely exchanging encryption keys between two parties is quantum key distribution (QKD), which ensures information-theoretic security by identifying any efforts at eavesdropping [2,3]. QKD is safe even against attackers with infinite computing power, in contrast to other cryptographic techniques that depend on computational complexity [4].

Numerous QKD techniques, including BB84 [5], E91 [5], and continuous variable QKD [6], have been developed throughout time. In order to expand the communication distance, decrease the quantum bit error rate, and enhance key rates, researchers have concentrated on refining these protocols [8]. New developments provide improved security and performance, such as twin-field QKD (TF-QKD) [10] and measurement-device-independent QKD (MDI-QKD) [9]. Researchers have also discovered weaknesses including detector blinding and photon-number-splitting assaults, which have prompted solutions like secure detectors [13] and the decoy-state technique [12].

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Research on integrating QKD into current communication networks has been quite active, especially in optical networks such as passive optical networks (PONs) and wavelength-division multiplexing (WDM) [14,15]. With the advent of the Key-as-a-Service (KaaS) idea, network operators may now effectively implement QKD-based security solutions [8]. In order to provide cryptographic methods that are safe against quantum attacks, post-quantum cryptography is being investigated concurrently. Among the potential methods being studied are lattice-based, code-based, and isogeny-based encryption [16,17,18].

In order to guarantee secure communication, quantum cryptography essentially depends on ideas like the Heisenberg uncertainty principle and quantum entanglement. Every effort at eavesdropping creates observable irregularities, warning the persons involved [3]. Secure key distribution is made possible by quantum entanglement, which guarantees that, even at great distances, the state of one particle influences that of its entangled counterpart. Because of this, quantum cryptography is an effective defense against new cybersecurity risks, especially in the age of quantum computing.

The increasing need for improved cybersecurity has drawn a lot of interest to the intersection of AI and quantum cryptography. By processing data and identifying patterns, AI may refine quantum cryptography methods, increasing their resilience and efficiency. In addition, quantum cryptography offers AI systems an impenetrable security architecture that guards against intrusions of private information and algorithms. Integrating artificial intelligence (AI) with quantum cryptography is becoming a crucial step toward future-proofing cybersecurity as quantum computers pose a threat to traditional cryptographic systems [19,20].

LITERATURE REVIEW

Cryptography means "secret writing" and is derived from the Greek terms kryptós, graphein, and logia [56]. Computational hardness assumptions are used in modern cryptography techniques to guarantee security [49]. These methods are often used in hash functions, digital payments, cybersecurity, cryptographic keys, and Zero-Knowledge Proofs (ZKP) [50]. Two encryption techniques that are based on older cryptographic models, such as the Data Encryption Algorithm (DEA), are the Triple Data Encryption Algorithm (3DEA) and the Advanced Encryption Standard (AES) [56], [68]. Rivest, Shamir, and Adleman's asymmetric RSA algorithm is another popular encryption method [53]. Sensitive data protection also heavily relies on legal frameworks like ISO 27001, GDPR, PCI-DSS, and NIST cybersecurity recommendations [42], [57], [61], [63], and [64]. New possibilities and difficulties are brought about by the development of quantum cryptography, especially in the areas of public key distribution and quantum-resistant encryption [48], [53], [55], and [66].

Cybersecurity is a major focus of current cryptographic research, and it's critical to comprehend the unique advantages and disadvantages of cryptographic applications in this field. Cryptography's efficacy depends on a number of important aspects. First and foremost, the encryption's strength is directly related to the difficulty of solving the underlying mathematical issue. Second, implementation is important; a bad implementation may weaken even the most robust algorithm. Third, it is crucial to keep cryptographic keys secret because they need to be safely kept, often by a centralized authority that can be trusted. One of these three areas—the mathematical challenge itself, implementation flaws, or secret key access—is probably where a hacker trying to compromise a cryptosystem will focus their efforts.

Although final standardization may not happen until late 2023, Ascon has been selected by the National Institute of Standards and Technology (NIST) as the standard for lightweight cryptography in low-memory IoT devices. Similar decisions have not yet been made by other organizations, such as ISO and ENISA, which may expose their IoT infrastructure. NIST highlighted the performance benefits of these new algorithms without sacrificing security, praising their efficacy. Given that NIST is a preeminent cybersecurity framework, this is significant. At first, 57 entries were submitted to the NIST lightweight cryptography competition. For the protection of data sent to and from a large number of tiny IoT devices, this kind of encryption is essential. These gadgets, which are often found in RFID tags and keyless entry systems, have less circuitry and power than more potent gadgets like cell phones. Their main benefits are their affordability and compact size, but these characteristics also place restrictions on more resource-intensive encryption methods now in use.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

The requirements of low-memory devices are met by lightweight encryption such as Ascon, while quantum cryptography provides an alternative strategy. With its emphasis on quantum key distribution (QKD) and potentially unbreakable security, it is based on quantum mechanics. While quantum cryptography uses qubits to provide secure communication independent of processing capacity, NIST's emphasis on Ascon seeks to safeguard data on resource-constrained IoT devices. The scalability and compatibility of quantum cryptography with present systems are major challenges. On the other hand, lightweight cryptography has to preserve security while using little processing power, which presents a problem for Internet of Things devices that are already restricted in this regard. Even more challenges may arise if quantum cryptography is directly implemented on these devices.

However, hybrid cryptography methods have emerged as a result of the fusion of conventional and quantum methodologies. These techniques improve security, even on low-power devices, by combining the advantages of both conventional and quantum systems. These hybrid algorithms may get beyond the drawbacks of traditional encryption and provide improved security levels that are essential in the modern digital world by using the special qualities of quantum physics.

To facilitate safe key exchange, quantum key distribution (QKD) techniques have been the subject of much study. Bennett and Brassard's groundbreaking BB84 technique [2] is still a fundamental and much researched example. Other protocols, such as continuous variable QKD [6] and E91 [5], have been developed as a result of further work, and they all use quantum mechanics to provide information-theoretic security [3].

Numerous QKD methods, such as BB84, E91, BBM92, B92, the Six-State Protocol, DPS, SARG04, COW, and S13, are covered in a survey by Nurhadi and Syambas [21]. Using a quantum simulator, they simulated BB84, B92, and BBM92 and found that BB84 had the greatest error probability and B92 the lowest. A modified BB84 protocol was presented by Kalra and Poonia [22], who showed that it had twice the capacity and almost half the error rate of the original. Their approach generates two keys for the sender and the recipient by using random bases for modulation and encoding. Using a single-photon source to create photon pulses, Sasaki et al. [23] presented a QKD mechanism that relies on quantum mechanics and eavesdropping detection for security. In order to obtain a 41dB channel loss tolerance and key speeds of 1.1bit/s and 300bit/s, respectively, Dirks et al. [24] combined untrusted and trusted mode BBM92 protocols to investigate the viability of a Geostationary Earth Orbit QKD system. Time synchronization and eavesdropper detection were shown by Williams et al. [25] via the implementation and testing of a time-bin encoding QKD algorithm using entangled photon pairs. To overcome entanglement deterioration at higher temperatures, Schimpf et al. [26] investigated the use of a polarization-entangled photon pair source that does not blink for QKD. In their analysis of quantum repeater QKD grid networks with few trusted nodes, Amer et al. [27] found constraints on the decoherence rate and BSM success probability. Ding et al. [28] suggested optimizing the parameters of a viable QKD system by employing the random forest method. In their evaluation of QKD and quantum bit commitment protocols, Dhoha et al. [29] concentrated on the BB84 QKD protocol's real-world application. A theoretical security analysis based on entropic uncertainty relations was presented by Yao et al. [30] in their discussion of the use of quantum random number generators and QKD protocols.

Numerous facets of post-quantum cryptography's (PQC) architecture, application, and security are being investigated. Side-channel attacks against Kyber, Saber, and NTRU were examined by Mujdei et al. [31], who also suggested a novel attack tactic that worked well even against randomization countermeasures. Their research highlights how side-channel vulnerabilities in PQC must be taken into consideration. Imana et al. [32] proposed two novel designs that increase area-time complexity and power efficiency in order to improve the efficiency of arithmetic operations inside InvBRLWE-based encryption. Their FPGA implementation and theoretical analysis point to possible uses in cryptoprocessors based on BRLWE/InvBRLWE. In order to improve security without compromising performance, Prakasan et al. [33] developed an authenticated-encryption technique using NTRU and Falcon to address security issues in the traditional channel of QKD. In conclusion, Sajimon et al. [34] assessed PQC algorithms for Internet of Things devices and suggested Kyber, Saber, Dilithium, and Falcon, with LightSaber-KEM and Dilithium2 being particularly recommended for quantum resistance. Future studies on quantum-resistant TLS and DTLS protocols for the Internet of Things may be based on their performance assessment using a Raspberry Pi 4.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Cryptography is undergoing a revolution thanks to AI and quantum computers. The goal of integrating AI with quantum cryptography is to use AI's capabilities to improve the security and efficiency of quantum cryptography systems. While quantum cryptography can safeguard AI systems, AI can enhance quantum protocols. In our data-driven society, where cyber risks are on the rise, this is essential. However, this integration is crucial due to the "quantum threat"—the potential for quantum computers to crack existing encryption. Quantum cryptography powered by AI aims to lessen this danger. The progress of AI and quantum cryptography, the problem of quantum computing, and the possibility of their combined strength for safe computation are all covered in this overview.

The "quantum threat" refers to the potential for future quantum computers to compromise existing cryptography systems. Quantum computers might effectively break methods like Shor's that depend on computationally challenging mathematical issues (such as factoring huge primes and elliptic curve discrete logarithms) like RSA and ECC. By using entanglement and superposition, quantum computers are able to do certain computations far more quickly than traditional computers. For example, Shor's algorithm puts existing encryption techniques at risk by enabling exponentially quicker factoring of big numbers. This is a growing reality rather than only a theoretical issue. Consequently, "post-quantum" or "quantum-resistant" cryptography—which employs methods that are inefficient for quantum computers to decipher—is essential. A strategic defense is provided by the combination of AI and quantum cryptography. AI can help create, test, and improve these new algorithms. It can also help analyze and adjust cryptographic systems in real time, making them more resilient to the advances in quantum computing. Thus, in the next quantum age, this convergence is essential to preserving data security.

Numerous investigations have examined security concerns and possible solutions within the framework of quantum and post-quantum encryption. The potential of quantum cryptography to improve cyberspace security was highlighted by Abidin et al. [35], who investigated the application of QKD and quantum cryptography in the DARPA Quantum Network for secure VPN communication. After reviewing post-quantum cryptography techniques for protecting IoT networks, Kumar et al. [36] came to the conclusion that safe and portable solutions for tiny devices are probably going to appear. In their analysis of the effects of quantum computing on DER networks, Ahn et al. [37] suggested the usage of PQC and QKD for protection and called for further study on high-performance, reasonably priced quantum-safe networks. Gupta et al. [38] identified potential for further study in blockchain with quantum countermeasures and presented a double-layered security mechanism for e-voting utilizing blockchain and QKD. Security flaws in CV-QKD were found by Lin et al. [39], who also suggested changes to the protocol and further research on security proofs. Cao et al. [40] showed that QKD may be used in practice by putting up a KaaS framework for incorporating it into optical networks. Lastly, Su et al. [41] provided fresh perspectives on QKD security by presenting a condensed information-theoretic security argument for the BB84 QKD protocol.

RESEARCH METHODOLOGY

This study examines the complex interaction between artificial intelligence (AI) and quantum cryptography using a qualitative research technique within an interpretative paradigm. Standardized tools and ontologies are essential for enhancing information sharing and automating vulnerability management as cybersecurity constantly changes. The "Reference Ontology for Cybersecurity Operational Information," which offers an organized framework for arranging cybersecurity data and promoting cooperation across businesses, is a noteworthy example [71]. This ontology ensures compatibility with industry standards while aiding in the structuring of cybersecurity information. This ontology was developed in close collaboration with cybersecurity firms, and its usefulness was evaluated by examining how well it conforms to industry standards. Furthermore, to facilitate cybersecurity knowledge bases and enhance information sharing, a flexible information structure was created [71].

The CYBEX framework, which attempts to standardize cybersecurity information sharing globally, is another noteworthy endeavor [72]. CYBEX, which was created as part of an ITU-T project, guarantees safe communication between cybersecurity organizations while preserving the accuracy of data exchanges. The use of this methodology helps to create a more consistent worldwide security posture and lessens the fragmentation of cybersecurity information. Information Description, Information Discovery, Information Query, Information

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Assurance, and Information Transport are the main functional blocks of CYBEX that are highlighted in this research. By automating procedures, reducing human error, and cutting expenses, these components improve cybersecurity operations.

Although they are not the main subject of this research, these frameworks are recognized for their importance in the larger cybersecurity environment [72], even though they have a substantial influence on cybersecurity information sharing and vulnerability management.

Considering international efforts to create and improve quantum-safe cryptographic algorithms, this study attempts to increase our understanding of how AI and quantum cryptography affect cybersecurity [65].

Data Collection

Two main approaches were used to obtain the data. First, recognized industry standards and recommendations, such as those published by NIST and ISO, were the source of original data [62], [64], and [68]. Additionally, a case study was carried out, which included speaking with specialists and the groups in charge of these standards directly.

For further study, these exchanges were methodically documented, transcribed, and categorized. Figure 1 provides a visual representation of the data collecting procedure.

Second, a thorough literature study was conducted with an emphasis on books and peer-reviewed journal papers. Research on encryption in the context of AI and quantum mechanics, particularly in relation to applications of quantum technology, received special attention [50], [55].

To provide a more comprehensive view, research on the effects of quantum technology on society was also included into the study [45], [47].

Data Analysis

The main technique used to investigate the relationships between national and international cybersecurity requirements was thematic analysis [54]. By methodically examining these interconnections and grouping the data into major themes, first coding was carried out [54].

In order to guarantee correctness and consistency, the coding procedure was meticulous and iterative, requiring ongoing data evaluation [54]. The theme analysis also included insights from scholarly literature, especially with reference to uses of quantum technology and its social ramifications [55].

Validation Procedures

The research used a triangulation method to assess software security using quantum computing techniques in order to guarantee the authenticity of the results. Cross-checking case study data insights with results from the body of existing research was part of this procedure.

Methodologies like the Hybrid Fuzzy ANP-TOPSIS Approach for software security evaluation [43], the durability perspective for quantum computing security [45], and the integrated hesitant fuzzy-based decision-making framework for sustainable and renewable energy assessments [46] were specifically taken into consideration. Peer-reviewed publications were also consulted to confirm important data points and analytical findings. These validation procedures were crucial in verifying that the study results were in line with recent developments in cybersecurity and in placing them within the larger academic discourse [45], [46].

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

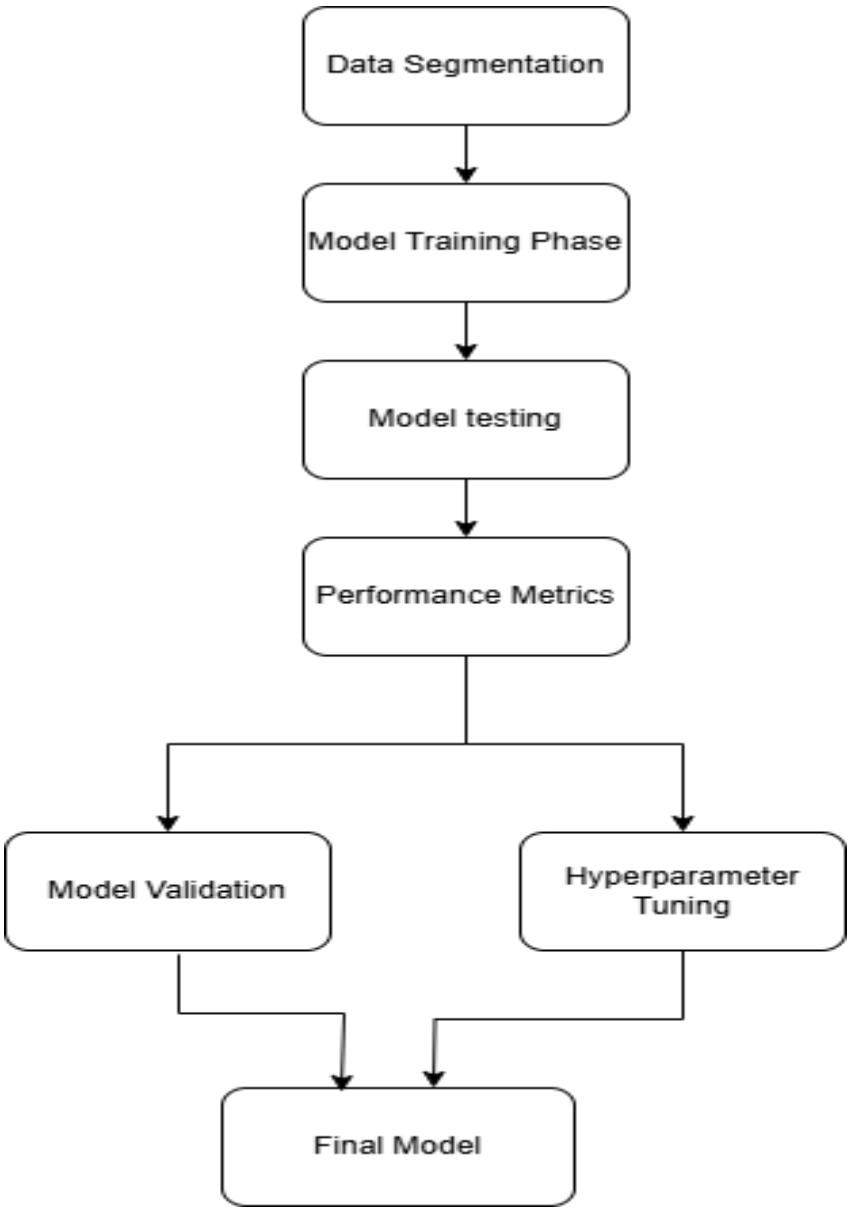


Figure 1. AI model evaluation and validation

The combination of quantum cryptography [72] with artificial intelligence [70] offers revolutionary opportunities for intelligent data processing and secure communication. This combination provides new ways to improve computational power and cybersecurity. In order to provide readers a better grasp of this intersection's effects on technology and security, this article examines its technological features, most current developments, and regulatory issues.

AI and Quantum Cryptography

S-boxes are an essential component of symmetric key algorithms in contemporary cryptography [56]. These structures are designed utilizing vectorial Boolean functions with the use of AI-driven methods, especially neural networks [72]. This method improves cryptographic security and expedites the development process [47]. Utilizing AI improves the efficiency and resilience of cryptographic protocols [70], which in turn fortifies cybersecurity frameworks [53].

Optimising Quantum Key Distribution (QKD)

A secure communication method called Quantum Key Distribution (QKD) uses the ideas of quantum physics to allow two parties to share cryptographic keys. The fundamental idea is based on the observation that any unwanted interception may be detected since measuring a quantum system changes its state by nature. Through

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

the transmission and measurement of quantum states, such photons, two parties—often referred to as Alice and Bob—create a shared key. They can detect any eavesdropper interference by examining their measurement data, and then use the key bits that are unaffected to create a safe encryption key. Although QKD offers complete security, guaranteeing that intercepted information cannot be decoded, it is operationally limited by communication speed and transmission distance.

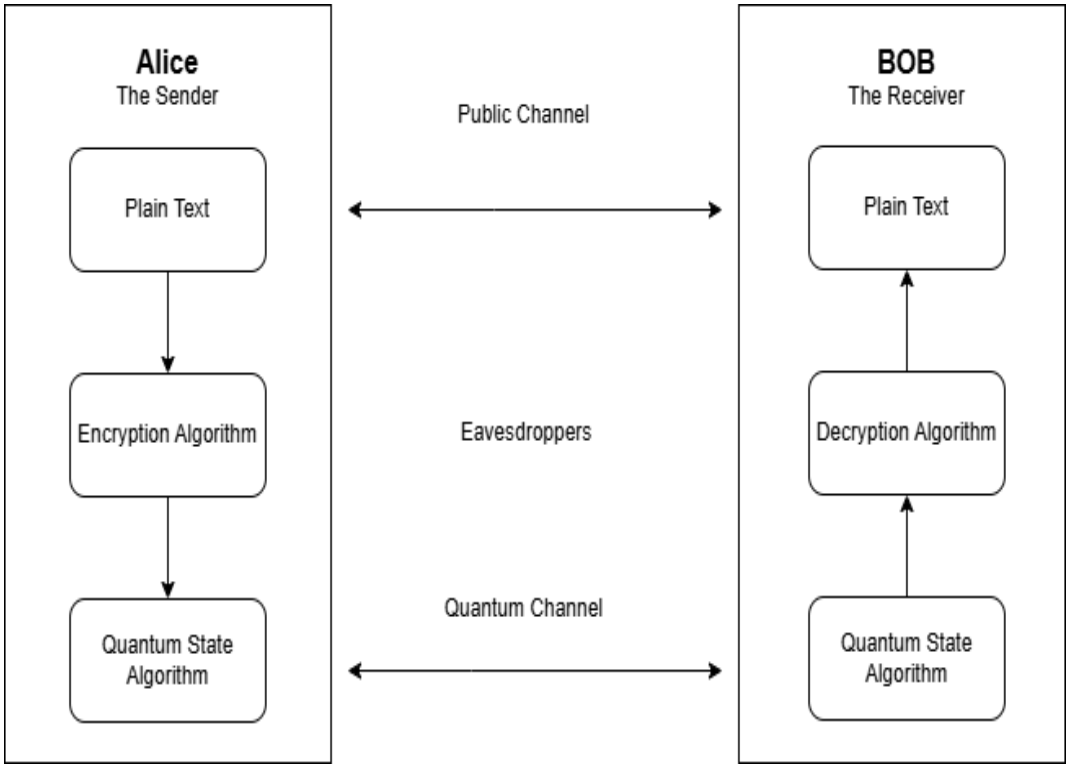


Figure 2. Basic Block Diagram of QKD System

Based on quantum physics, quantum cryptography—where two people exchange a shared secret key—allows rather strong communication via QKD (Quantum Key Distribution). One prominent QKD protocol is BB84 [72]. Even although QKD is very safe, mistakes and other security risks still exist. There are various ways AI may improve QKD. It guarantees communication security, preserves important integrity, and predicts and fixes mistakes, thereby helping in error correction. By spotting efforts at eavesdropping or security breaches, AI-driven monitoring strengthens system security. Moreover, artificial intelligence can maximize quantum key generating rates [70] by considering hardware and ambient factors for higher efficiency. These developments make QKD more dependable and safe, therefore guaranteeing strong future communication.

Securing AI with Quantum Cryptography: Principles, Applications, and Regulations

Industries using artificial intelligence have to give security first priority in order to guard algorithms and private information against leaks that can cause financial losses or damage to reputation. Quantum cryptography delivers a solid security layer by employing quantum physics, rendering data intrusions computationally infeasible. Implementing these strategies boosts AI systems' safety and integrity, guaranteeing dependable data processing.

Quantum mechanics brings ideas unique from classical physics, which motivates developments in artificial intelligence. Quantum entanglement, for example, optimises AI algorithms by boosting neural network training efficiency [70]. This invention encourages the creation of quicker, more powerful AI models capable of processing information in novel ways.

The integration of AI with quantum cryptography raises regulatory issues [71], demanding worldwide cooperation to set security standards. Organisations like ISO, IEC, and NIST have built frameworks to assure the security and reliability of quantum cryptography systems [72]. Additionally, legislation such as GDPR

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

increase openness and responsibility in AI decision-making. Addressing these issues demands collaboration among academia, politicians, and business leaders to fully utilize AI-quantum integration while ensuring security and regulatory compliance

Challenges and Opportunities

Integrating AI and Quantum Cryptography

The confluence of AI and quantum cryptography brings breakthrough prospects but also raises substantial problems. AI, especially neural networks, has shown considerable promise in enhancing cryptographic systems. One significant use is the optimisation of S-boxes in symmetric key cryptography, such as AES, where AI-driven algorithms boost security by enhancing nonlinearity and differential uniformity. Additionally, AI-based cryptanalysis may reveal flaws in encryption methods by training models to anticipate keys or decrypt communications without them.

Beyond standard encryption, AI is vital in tackling risks presented by quantum computing. Quantum algorithms like Shor's algorithm may effectively factor big numbers, weakening RSA encryption, while quantum capabilities also endanger ECC and Diffie-Hellman protocols. The concepts of quantum superposition and entanglement enable quantum computers to do computations exponentially faster than conventional systems, rendering present encryption approaches obsolete. To overcome these weaknesses, AI assists in modeling quantum assaults and improving post-quantum cryptography methods, providing safe data security in the quantum age.

Technological and Data Challenges

Despite its potential, combining AI with quantum cryptography systems involves technical challenges. Quantum hardware development and error correction need major breakthroughs, especially for distributed quantum systems. Additionally, AI-driven quantum cryptography relies on large-scale data encryption, raising questions regarding scalability, privacy, and biases. The significant infrastructural expenses and processing needs of quantum systems further hamper mainstream implementation.

Real-time applications demand minimum latency, although AI and quantum cryptography processes might create delays, limiting usability in time-sensitive contexts. Furthermore, quantum cryptography systems are particularly susceptible to external variables, which may lead to increasing mistake rates, compromising their dependability and accuracy across varied settings.

Opportunities for Enhanced Security Mechanisms and AI-Driven Quantum Systems

The prospective merging of AI's outstanding data processing skills with the impregnable security of quantum encryption might give birth to ultra-secure communication routes impenetrable to classical and quantum attacks. With the fast improvements in quantum computing, accumulating evidence implies that quantum systems may soon outperform conventional systems regarding computational capabilities [47]. AI has the potential to greatly improve quantum systems, leading to speedier algorithms and simplified cryptographic protocols with far-reaching effects. Such breakthroughs potentially change secure communication and data sharing. The combination of quantum notions with artificial intelligence holds promise for new study areas, drawing increasingly substantial funding in quantum cryptography and pushing the frontiers of both domains.

There are considerable obstacles when integrating AI with quantum cryptography, but the potential benefits are huge. Researchers may unearth a variety of options that create the basis for future improvements in computing and security. These improvements can change how we approach these professions and dramatically influence society.

Public key (PK) cryptography plays a critical part in this endeavor. Asymmetric cryptography, or public key (PK) cryptography, employs two mathematically connected keys: public and private. Unlike symmetric cryptography, which depends on one key for encryption and decryption, PK cryptography requires different keys

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

for each operation. This strengthens security and guarantees that sensitive data remains protected, even if an opponent intercepts the public key. PK cryptography offers secure communication and cryptographic features such as crucial exchanges, digital signatures, and data encryption. It is a fundamental component of current cryptographic systems, giving greater security, scalability, and flexibility across many applications.

A key idea in cryptography is digital signature creation. To construct a digital signature, the signatory must first build a key pair consisting of a private key and a public key. The private key is kept secret and never disclosed, but the public key is made accessible. A unique hash of the document or communication to be signed is created using a hash function. This hash value uniquely reflects the content of the document. Hash signing happens when the signer encrypts the resulting hash value using their private key. This relates their signature to a certain paper. Upon encrypting the hash value, a cryptographic digital signature is formed, unique to both the document and the signer.

Future Prospects and the Path Forward

Despite these obstacles, AI plays a significant role in strengthening quantum cryptography protocols, boosting flexibility and efficiency. AI-driven tactics have efficiently reduced quantum risks and encouraged the development of quantum-resistant cryptographic systems, enabling secure communications and data security across sectors. However, additional research and development are essential to enhance scalability, minimize latency, and integrate quantum security technologies with current infrastructures.

Standardisation, regulatory frameworks, and industry cooperation are necessary to a smooth transition to quantum-secure cryptographic systems. Efforts should concentrate on building strong, generally recognized quantum-resistant solutions while promoting relationships between academics, business, and government. As quantum computing becomes a reality, establishing robust post-quantum cryptography frameworks will be vital in securing digital assets and maintaining long-term cybersecurity resilience.

The combination of AI and quantum cryptography brings fascinating prospects. Despite the considerable hurdles that must be overcome, the potential benefits are immense, and the ramifications might be far-reaching. Merging these two domains may open a variety of possibilities that set the basis for future improvements in computing and security. This might revolutionize secure communication and data transport, leading to new study areas and pushing the frontiers of both domains.

Artificial Intelligence in Cryptographyn

Overview of AI Techniques in Cryptography

Artificial Intelligence (AI) has substantially affected cryptography applications by employing machine learning methods to better encryption and cryptanalysis [71]. Neural networks, in particular, increase cryptographic security by recognizing patterns and anticipating flaws in encrypted data. AI also enhances cryptographic protocols by increasing anomaly detection and decreasing computing complexity [72].

AI in Classical Cryptography

AI is vital in cryptanalysis, where machine learning models evaluate encrypted data to anticipate encryption keys and find abnormalities. By enhancing standard encryption approaches, AI helps fight brute-force assaults and boosts security [46]. The symbiotic link between AI and encryption assures continuing breakthroughs in both domains, supporting safe communications and data security [44].

AI in Quantum Cryptography

The incorporation of AI into quantum cryptography brings both potential and problems [45]. With the introduction of quantum computing, standard encryption techniques have greater weaknesses. AI-driven models help uncover flaws and enhance quantum key distribution (QKD) approaches, ultimately boosting security

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

against quantum attacks [50]. AI also advances quantum cryptography systems by assessing quantum noise and error correction, guaranteeing dependable communication routes [66].

Quantum Cryptography

Principles of Quantum Cryptography

Quantum cryptography draws its security from quantum physics, specifically the no-cloning theorem, which precludes replication of quantum states. This essential concept assures the integrity of quantum cryptography systems [48].

Quantum Key Distribution

Quantum Key Distribution (QKD) enables two parties to distribute cryptographic keys safely by exploiting quantum physics [60]. The BB84 protocol is one of the most extensively used QKD algorithms, intended to identify eavesdropping attempts. If an unauthorized party intercepts quantum keys, disruptions in the quantum states signify possible security breaches [52].

Quantum Cryptographic Protocols

Beyond QKD, quantum cryptographic algorithms include quantum digital signatures, quantum coin flipping, and quantum secure direct communication, each giving increased security features that classical cryptography cannot accomplish [50].

Challenges and Solutions

Quantum cryptography confronts various problems, including hardware restrictions, quantum noise, and channel loss [66]. Researchers are tackling these difficulties using post-quantum cryptography (PQC), which attempts to design algorithms immune to quantum assaults [65].

Intersection of AI and Quantum Cryptography

Synergistic Approaches

The merging of AI with quantum cryptography opens new possibilities for safe computing. AI helps enhance quantum encryption processes, making cryptographic systems more efficient and immune to cyber assaults [58].

AI-Enhanced Quantum Cryptographic Protocols

AI-driven models boost QKD security by evaluating quantum states and anticipating eavesdropping attempts [48]. AI also helps to the development of post-quantum cryptography algorithms, guaranteeing resistance against quantum cyber attacks [55].

Quantum Computing for AI Model Security

Quantum computing increases AI security by allowing better encryption approaches based on qubits, which enable higher-dimensional computational spaces for more resilient cryptographic models [67].

Potential Risks and Mitigation Strategies

The fast development of AI-driven quantum cryptography raises possible security vulnerabilities. Ethical concerns and ongoing monitoring are important to balance innovation with risk minimization [64].

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Applications and Implications

The combination of AI and quantum computing has led to advancements in cybersecurity, financial security, and healthcare data protection [59]. Quantum AI enhances encryption methods, making them more resistant to attacks [68]. Additionally, quantum computing has applications in biochemical research, enabling more efficient simulations of molecular interactions [59].

Despite its advantages, quantum-AI integration poses privacy risks. Policymakers must establish regulatory frameworks to address data security concerns and ensure responsible technological development [61].

Case Studies: AI and Quantum Cryptography Integration

AI in Quantum Cryptographic Systems

The combination of AI with quantum cryptography techniques has resulted in sophisticated encryption approaches capable of fighting emerging cyber threats [46]. AI-driven encryption helps enterprises to safeguard critical data and boost cybersecurity frameworks [55].

Real-World Applications and Outcomes

Quantum AI has increased transaction security in the banking sector by reinforcing cryptographic protocols. AI-based cybersecurity solutions, such as the CS-FSM approach and the K-nearest neighbor (KNN) algorithm, identify and prevent malware assaults while boosting data protection [43]. In the retail industry, AI-powered quantum encryption preserves the secrecy of consumer transactions, offering a solid defense against cyber attacks [72].

Transitioning to quantum cryptography systems involves implementation hurdles, but strategic planning may assist overcome these barriers. The merger of AI with quantum cryptography delivers major advantages in cybersecurity, banking, and secure communication, influencing the future of data protection.

DISCUSSION

The Convergence of AI and Quantum Cryptography: A New Era of Secure Communication

The combination of AI and quantum physics in cryptography systems has the potential to transform data security and transaction protection across sectors. This combination boosts cryptographic resistance against upcoming cyber threats while allowing the creation of quantum-resistant algorithms and enhanced security frameworks. As quantum computing improves, AI-driven quantum cryptography will be important in securing sensitive information and guaranteeing secure communication.

Quantum Key Distribution (QKD) and Post-Quantum Cryptography

Quantum Key Distribution (QKD) methods such as BB84, E91, and B92 employ quantum mechanics to assure safe key exchange. While these protocols provide information-theoretic security, difficulties relating to efficiency, scalability, and vulnerability to assaults persist. Further study is essential to improve these protocols for practical implementation in real-world quantum networks.

Post-quantum cryptography focuses on building encryption methods resistant to quantum assaults. Techniques such as lattice-based, code-based, and isogeny-based cryptography offer promise in safeguarding digital communications beyond conventional encryption. However, assuring their efficiency, security, and acceptance needs continual inquiry and development.

Integrating QKD into Optical Networks

The implementation of QKD in optical networks, including Key-as-a-Service (KaaS) models, has permitted the deployment of quantum-secured communications inside existing infrastructures. Despite its promise, integration

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

difficulties like as cost, downsizing, and compatibility with older systems must be overcome to permit large-scale adoption. Overcoming these limitations will be key in promoting QKD as a popular security solution.

Addressing Security Threats and Countermeasures

Despite its inherent security benefits, quantum cryptography confronts dangers such as quantum hacking, side-channel attacks, and implementation weaknesses. Countermeasures include decoy state approaches, entanglement-based QKD, privacy amplification, and quantum coin flipping procedures have been suggested to alleviate these hazards. Ongoing research is necessary to strengthen the resilience of quantum security systems against emerging cyber threats.

AI-Powered Quantum Cryptography and Industry Applications

AI-driven quantum cryptography has the potential to alter sectors such as banking, e-commerce, healthcare, national security, and telecommunications by delivering adaptive and intelligent security mechanisms. AI advances quantum cryptography approaches by optimizing key management, detecting threats in real time, and boosting system efficiency. The deployment of these technologies may dramatically boost data privacy and enhance customer confidence.

However, ethical problems concerning data privacy, algorithmic prejudice, and possible exploitation must be properly addressed. Sustainable and adaptive cryptographic procedures must be created to keep pace with continuing breakthroughs in AI and quantum computing. Policymakers should develop legislative frameworks that stimulate innovation while assuring ethical usage and security.

Future Prospects and Global Collaboration

The future of AI-powered quantum cryptography hinges on cooperation between academics, industry leaders, and regulators. Continued investment in research, worker training, and policy development is crucial for increasing adoption and promoting innovation. Establishing global standards and best practices will be important to guaranteeing smooth integration and interoperability across diverse industries.

As AI and quantum cryptography continue to improve, their combined potential provides a disruptive approach to cybersecurity. By bolstering encryption, minimizing quantum-era dangers, and constructing a safe digital environment, these technologies will influence the future of global data security. With persistent research and worldwide collaboration, AI-driven quantum cryptography will revolutionize how sensitive information is safeguarded in the quantum computing age.

CONCLUSION

The combination of AI with quantum cryptography has the potential to greatly advance cryptographic systems and security measures. This integration has already led to substantial breakthroughs in industries like banking and e-commerce, allowing the establishment of strong security procedures and increasing customer confidence. The field of AI-driven quantum cryptography is rapidly evolving, with key areas of innovation including hybrid cryptographic systems, automated cryptographic protocol design, quantum key distribution (QKD) enhancements, post-quantum cryptography development, quantum machine learning for cryptanalysis, and secure multi-party computation (MPC).

The promise of quantum cryptography in changing digital communication in the quantum age is tremendous, but various hurdles and outstanding research topics must be solved. Focused research on robust QKD protocols, safe post-quantum cryptographic algorithms, and efficient solutions for IoT devices is necessary to allow secure and practical quantum cryptography applications.

AI-powered optimization and analysis may be crucial in building and fine-tuning hybrid systems for optimal efficiency and security. AI technologies like as machine learning and neural networks are showing very promise in the automated construction of cryptographic protocols.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

In conclusion, the combination of AI with quantum cryptography offers a very promising topic with considerable potential to better data security and privacy.

REFERENCES

1. L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proceedings of the twentyeighth annual ACM symposium on Theory of computing, pp. 212–219, 1996.
2. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," arXiv preprint arXiv:2003.06557, 2020.
3. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusˇek, N. Lu¨tkenhaus, and M. Peev, "The security of practical quantum key distribution," Reviews of modern physics, vol. 81, no. 3, p. 1301, 2009.
4. H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," Journal of Cryptology, vol. 18, pp. 133–165, 2005.
5. A. K. Ekert, "Quantum cryptography based on bell's theorem," Physical review letters, vol. 67, no. 6, p. 661, 1991.
6. C. Weedbrook, S. Pirandola, R. Garc´ıa-Patro´n, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," Reviews of Modern Physics, vol. 84, no. 2, p. 621, 2012.
7. S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weed- brook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Ja- cobsen, and U. L. Andersen, "High-rate measurement- device-independent quantum cryptography," Nature Photonics, vol. 9, no. 6, pp. 397–402, 2015.
8. S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, et al., "Field and long-term demonstration of a wide area quantum key distribution network," Optics express, vol. 22, no. 18, pp. 21739–21756, 2014.
9. H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," Nature Photonics, vol. 8, no. 8, pp. 595–604, 2014.
10. M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," Na- ture, vol. 557, no. 7705, pp. 400–403, 2018.
11. Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key- distribution systems," Physical Review A, vol. 78, no. 4, p. 042333, 2008.
12. W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," Physical review letters, vol. 91, no. 5, p. 057901, 2003.
13. D. Elser, K. Gunthner, I. Khan, B. Stiller, C. Mar- quardt, G. Leuchs, K. Saucke, D. Trondle, F. Heine, S. Seel, et al., "Satellite quantum communication via the alphasat laser communication terminal-quantum signals from 36 thousand kilometers above earth," in 2015 IEEE international conference on space optical systems and applications (ICSOS), pp. 1–4, IEEE, 2015.
14. I. Derkach, V. C. Usenko, and R. Filip, "Continuous- variable quantum key distribution with a leakage from state preparation," Physical Review A, vol. 96, no. 6, p. 062309, 2017.
15. R. Kumar, H. Qin, and R. Alle´aume, "Coexistence of continuous variable qkd with intense dwdm classical channels," New Journal of Physics, vol. 17, no. 4, p. 043027, 2015.
16. D. J. Bernstein, T. Lange, and P. Schwabe, "The security impact of a new cryptographic library," in Progress in Cryptology–LATINCRYPT 2012: 2nd International Conference on Cryptology and Information Security in Latin America, Santiago, Chile, October 7-10, 2012. Proceedings 2, pp. 159–176, Springer, 2012.
17. M. Mosca, "Cybersecurity in an era with quantum computers: will we be ready?," IEEE Security & Privacy, vol. 16, no. 5, pp. 38–41, 2018.
18. D. Jao and L. De Feo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," in Post-Quantum Cryptography: 4th Inter- national Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011. Proceedings 4, pp. 19–34, Springer, 2011.
19. N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," Reviews of Modern Physics, vol. 83, no. 1, p. 33, 2011.
20. M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita,
21. Z. Wang, A. Tanaka, et al., "Field test of quantum key distribution in the Tokyo qkd network," Optics express, vol. 19, no. 11, pp. 10387–10409, 2011.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

22. A. I. Nurhadi and N. R. Syambas, "Quantum key distribution (qkd) protocols: A survey," in 2018 4th International Conference on Wireless and Telematics (ICWT), pp. 1–5, IEEE, 2018.
23. M. Kalra and R. C. Poonia, "Design a new protocol and compare with bb84 protocol for quantum key distribution," in Soft Computing for Problem Solving: SocProS 2017, Volume 2, pp. 969–978, Springer, 2019.
24. T. Sasaki, Y. Yamamoto, and M. Koashi, "Practical quantum key distribution protocol without monitoring signal disturbance," Nature, vol. 509, no. 7501, pp. 475–478, 2014.
25. B. Dirks, I. Ferrario, A. Le Pera, D. V. Finocchiaro, M. Desmons, D. de Lange, H. de Man, A. J. Meskers, J. Morits, N. M. Neumann, et al., "Geoqkd: quantum key distribution from a geostationary satellite," in International Conference on Space Optics—ICSO 2020, vol. 11852, pp. 222–236, SPIE, 2021.
26. J. Williams, M. Suchara, T. Zhong, H. Qiao, R. Ket- timuthu, and R. Fukumori, "Implementation of quantum key distribution and quantum clock synchroniza- tion via time bin encoding," in Quantum Computing, Communication, and Simulation, vol. 11699, pp. 16– 25, SPIE, 2021.
27. C. Schimpf, S. Manna, S. F. Covre da Silva, M. Aigner, and A. Rastelli, "Entanglement-based quantum key distribution with a blinking-free quantum dot operated at a temperature up to 20 k," Advanced Photonics, vol. 3, no. 6, pp. 065001–065001, 2021.
28. O. Amer, W. O. Krawec, and B. Wang, "Efficient routing for quantum key distribution networks," in 2020 IEEE International Conference on Quantum Computing and Engineering (QCE), pp. 137–147, IEEE, 2020.
29. H.-J. Ding, J.-Y. Liu, C.-M. Zhang, and Q. Wang, "Predicting optimal parameters with random forest for quantum key distribution," Quantum Information Processing, vol. 19, pp. 1–8, 2020.
30. A.-M. Dhoha, A.-K. Mashael, A.-A. Ghadeer, A.- A. Manal, M. Al Fosail, and N. Nagy, "Quantum cryptography on ibm qx," in 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), pp. 1–6, IEEE, 2019.
31. K. Yao, W. O. Krawec, and J. Zhu, "Quantum sam- pling for finite key rates in high dimensional quantum cryptography," IEEE Transactions on Information Theory, vol. 68, no. 5, pp. 3144–3163, 2022.
32. C. Mujdei, L. Wouters, A. Karmakar, A. Beckers, J. M. B. Mera, and I. Verbauwhede, "Side-channel analysis of lattice-based post-quantum cryptography: Exploiting polynomial multiplication," ACM Transac- tions on Embedded Computing Systems, 2022.
33. J. L. Iman˜a, P. He, T. Bao, Y. Tu, and J. Xie, "Efficient hardware arithmetic for inverted binary ring-lwe based post-quantum cryptography," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 69, no. 8, pp. 3297–3307, 2022.
34. A. Prakasan, K. Jain, and P. Krishnan, "Authenticated- encryption in the quantum key distribution classical channel using post-quantum cryptography," in 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 804–811, IEEE, 2022.
35. P. Sajimon, K. Jain, and P. Krishnan, "Analysis of post-quantum cryptography for internet of things," in 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 387– 394, IEEE, 2022.
36. S. Abidin, A. Swami, E. Ramirez-As´ıs, J. Alvarado- Tolentino, R. K. Maurya, and N. Hussain, "Quantum cryptography technique: A way to improve security challenges in mobile cloud computing (mcc)," Materials Today: Proceedings, vol. 51, pp. 508–514, 2022.
37. A. Kumar, C. Ottaviani, S. S. Gill, and R. Buyya, "Securing the future internet of things with post- quantum cryptography," Security and Privacy, vol. 5, no. 2, p. e200, 2022.
38. J. Ahn, H.-Y. Kwon, B. Ahn, K. Park, T. Kim, M.- K. Lee, J. Kim, and J. Chung, "Toward quantum secured distributed energy resources: Adoption of post-quantum cryptography (pqc) and quantum key distribution (qkd)," Energies, vol. 15, no. 3, p. 714, 2022.
39. S. Gupta, A. Gupta, I. Y. Pandya, A. Bhatt, and K. Mehta, "End to end secure e-voting using blockchain & quantum key distribution," Materials Today: Proceedings, 2021.
40. Y.-Q. Lin, M. Wang, X.-Q. Yang, and H.-W. Liu, "Counterfactual quantum key distribution with untrusted detectors," Heliyon, vol. 9, no. 2, 2023.
41. Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "Kaas: Key as a service over quantum key distribution integrated optical networks," IEEE Communications Magazine, vol. 57, no. 5, pp. 152–159, 2019.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

42. H.-Y. Su, "Simple analysis of security of the bb84 quantum key distribution protocol," Quantum Information Processing, vol. 19, no. 6, p. 169, 2020.
43. Advisera, "What is the meaning of ISO 27001?" [Online]. Available: https://advisera.com/27001academy/what-is-iso-27001/.
44. A. Agrawal et al., "Software security estimation using the hybrid fuzzy ANP-TOPSIS approach: design tactics perspective," Symmetry, vol. 12, no. 4, p. 598, 2020, doi: 10.3390/SYM12040598.
45. A. Aldoseri, K. N. Al-Khalifa, and A. M. Hamouda, "Re-thinking data strategy and integration for artificial intelligence: concepts, opportunities, and challenges," Appl. Sci., vol. 13, no. 12, p. 7082, 2023, doi: 10.3390/APP13127082.
46. H. Alyami et al., "The evaluation of software security through quantum computing techniques: a durability perspective," Appl. Sci., vol. 11, no. 24, p. 11784, 2021, doi: 10.3390/APP112411784.
47. U. Awan, L. Hannola, A. Tandon, R. K. Goyal, and A. Dhir, "Quantum computing challenges in the software industry. A fuzzy AHP-based approach," Inf. Softw. Technol., vol. 147, p. 106896, 2022, doi: 10.1016/J.INFSOF.2022.106896.
48. O. Ayoade, P. Rivas, and J. Orduz, "Artificial intelligence computing at the quantum level," Data, vol. 7, no. 3, p. 28, 2022, doi: 10.3390/DATA7030028.
49. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," Theor. Comput. Sci., vol. 560, no. P1, pp. 7–11, 2020, doi: 10.1016/j.tcs.2014.05.025.
50. M. Braverman, Y. K. Ko, and O. Weinstein, "Approximating the best Nash equilibrium in no (1ogn)-time breaks the exponential time hypothesis," Proc. West Mark Ed Assoc Conf., vol. 2015, no. January, pp. 970–982, 2015, doi: 10.1137/1.9781611973730.66.
51. A. Broadbent and C. Schaffner, "Quantum cryptography beyond quantum key distribution," Des. Codes Cryptogr., vol. 78, no. 1, pp. 351–382, 2015, doi: 10.1007/S10623-015-0157-4.
52. J. E. Catril Opazo, "NIST cybersecurity framework in South America: Argentina, Brazil, Chile, Colombia, and Uruguay," 2021.
53. E. Diamanti, H. K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," NPJ Quantum Inf., vol. 2, no. 1, pp. 1–12, 2016, doi: 10.1038/npjqi.2016.25.
54. W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory, vol. 22, no. 6, pp. 644–654, 1976, doi: 10.1109/TIT.1976.1055638.
55. K. M. Eisenhardt, "Building theories from case study research," Acad. Manag. Rev., vol. 14, no. 4, p. 532, 1989, doi: 10.2307/258557.
56. A. Elaziz and F. Raheman, "The future of cybersecurity in the age of quantum computers," Fut. Internet, vol. 14, no. 11, p. 335, 2022, doi: 10.3390/FI14110335.
57. H. Feistel, "Block cipher cryptographic system," 1971.
58. GDPR, "What is GDPR, the EU's new data protection law?" [Online]. Available: https://gdpr.eu/what-is-gdpr/.
59. S. S. Gill et al., "AI for next-generation computing: Emerging trends and future directions," Internet of Things, vol. 19, p. 100514, 2022, doi: 10.1016/J.IOT.2022.100514.
60. S. Gupta, S. Modgil, P. C. Bhatt, C. J. Chiappetta Jabbour, and S. Kamble, "Quantum computing-led innovation for achieving a more sustainable Covid-19 healthcare industry," Technovation, vol. 120, p. 102544, 2023, doi: 10.1016/J.TECHNOVATION.2022.102544.
61. L. Gyongyosi and S. Imre, "Secret key rate adaption for multicarrier continuous-variable quantum key distribution," SN Comput. Sci., vol. 1, no. 1, pp. 1–17, 2020, doi: 10.1007/s42979-019-0027-7.
62. ICO, "Information Commissioner's Office (ICO): The UK GDPR, UK GDPR guidance and resources," [Online]. Available: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/.
63. ISO, "ISO/IEC 27035–1:2016—Information technology—Security techniques—Information security incident management—Part 1: Principles of incident management," [Online]. Available: https://www.iso.org/standard/60803.html.
64. ISO, "ISO/IEC 27001 and related standards Information security management," 2022.
65. C. Johnson, L. Badger, D. Waltermire, J. Snyder, and C. Skorupka, "Guide to cyber threat information sharing," NIST Spec. Publ., 2016, doi: 10.6028/NIST.SP.800-150.
66. M. Kumar, "Post-quantum cryptography algorithm's standardization and performance analysis," Array, vol. 15, p. 100242, 2022, doi: 10.1016/J.ARRAY.2022.100242.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

67. V. Lovic, “Quantum key distribution: advantages, challenges and policy,” 2020, doi: 10.17863/CAM.58622.
68. G. M. Mallow et al., “Quantum computing: the future of big data and artificial intelligence in spine,” Spine Surg. Relat. Res., vol. 6, no. 2, p. 93, 2022, doi: 10.22603/SSRR.2021-0251.
69. NIST, “Advanced Encryption Standard (AES),” 2001. [Online]. Available: https://web.archive.org/web/20170312045558/http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.
70. A.-M. Udroiu, M. Dumitrache, and I. Sandu, “Improving the cybersecurity of medical systems by applying the NIST framework,” in Proc. 14th Int. Conf. Electron. Comput. Artif. Intell. (ECAI), IEEE, 2022, pp. 1–7.
71. M. Ying, “Quantum computation, quantum theory, and AI,” Artif. Intell., vol. 174, no. 2, pp. 162–176, 2010, doi: 10.1016/J.ARTINT.2009.11.009.
72. Radanliev, P. Artificial intelligence and quantum cryptography. J Anal Sci Technol 15, 4 (2024). https://doi.org/10.1186/s40543-024-00416-6
73. M. S. Akter, J. Rodriguez-Cardenas, H. Shahriar, A. Cuzzocrea and F. Wu, "Quantum Cryptography for Enhanced Network Security: A Comprehensive Survey of Research, Developments, and Future Directions," 2023 IEEE International Conference on Big Data (BigData), Sorrento, Italy, 2023, pp. 5408-5417, doi: 10.1109/BigData59044.2023.10386889.

ABOUT THE AUTHORS



Mr. **Hemant N. Chaudhari** is currently pursuing PhD in Computer Science and Engineering, Mahakaushal University, Jabalpur. And he is an Assistant Professor in Department of CSE [Cyber Security] at G H R College of Engineering and Management, Wagholi, Pune. He received his BE degree in Information Technology from NMU, Jalgaon in 2008 and MTech degree in Software Engineering from RGPV, Bhopal in 2014