

Paper Type: Original Article

# Harnessing Quantum Computing and Artificial Intelligence for Next-Generation Cybersecurity: A Comprehensive Review

Kaosar Hossain\*

Doctors of Management, International American University, USA; Mkhs795@gmail.com.

Citation:

|                             |   |
|-----------------------------|---|
| Received: 25 March 2025     | Hossain, K. (2025). Harnessing quantum computing and artificial intelligence for next-generation cybersecurity: A comprehensive review. <i>Soft computing fusion with applications</i> , 2(4), 203-218. |
| Revised: 10 July 2025       |   |
| Accepted: 05 September 2025 |   |

## Abstract


The rapid escalation of cyber threats has revealed the limitations of traditional security frameworks and encryption methods. Advances in quantum computing are expected to undermine widely used cryptographic systems, creating the need for more resilient approaches. This paper reviews the combined role of quantum computing and Artificial Intelligence (AI) in shaping the future of cybersecurity. By leveraging principles such as superposition, entanglement, and interference, quantum systems offer unmatched computational capabilities that can support post-quantum cryptography (PQC) and advanced security models. Simultaneously, AI enhances anomaly detection and enables adaptive encryption management, strengthening defenses against evolving attacks. The discussion explores quantum-resistant algorithms, secure communication techniques such as Quantum Key Distribution (QKD), and hybrid quantum–AI systems for protecting critical infrastructures. Ethical and regulatory considerations are also highlighted to ensure responsible and equitable adoption of these technologies. Overall, the paper underscores how the integration of quantum advancements with intelligent systems can transform cybersecurity by enhancing resilience, safeguarding sensitive data, and fostering digital trust in an era of rapid technological change.

**Keywords:** Quantum computing, Cybersecurity, Post-quantum cryptography, Quantum key distribution, Secure communication.

## 1 | Introduction

In the contemporary digital age, the rapid proliferation of interconnected technologies has amplified both the opportunities and vulnerabilities of global information systems. Organizations, governments, and individuals now rely heavily on digital infrastructures to manage sensitive information, including financial transactions, healthcare data, energy operations, and national defense systems. This dependence has created an unprecedented scale of exposure to cyber threats such as ransomware, phishing schemes, supply chain compromises, and state-sponsored intrusions, which continue to grow in complexity and frequency [1], [2].

 Corresponding Author: Mkhs795@gmail.com

 <https://doi.org/10.22105/scfa.vi.75>



Licensee System Analytics. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

Traditional security frameworks, developed on classical computational models, are increasingly strained in their ability to counter such threats effectively. The accelerating pace of digital transformation—driven by the Internet of Things (IoT), cloud platforms, big data ecosystems, and smart grids—has expanded the attack surface and heightened vulnerabilities across sectors [3]–[5]. These developments have transformed cybersecurity from a purely technical issue into a strategic concern with economic, social, and geopolitical consequences [6]. The escalating cost of cybercrime, measured in financial losses, service disruptions, and the erosion of public trust, underscores the urgency for transformative solutions [7], [8]. Within this evolving landscape, emerging technologies such as quantum computing and Artificial Intelligence (AI) have begun to attract attention as potential disruptors, capable of reshaping cybersecurity by providing computational power and adaptive intelligence that classical methods cannot match [9], [10].

Despite remarkable advancements in conventional cybersecurity measures, the foundations of current encryption and defense systems are increasingly fragile in the face of disruptive technological change. Classical cryptographic methods such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) depend on the computational difficulty of factoring large integers or solving discrete logarithm problems; however, quantum algorithms such as Shor's algorithm are expected to dismantle these assumptions with relative ease, leaving widely deployed systems vulnerable to compromise [11]. The anticipated rise of scalable quantum computers, therefore, poses a profound threat to the confidentiality and integrity of encrypted data across financial, healthcare, and governmental domains [10]. At the same time, AI has demonstrated significant progress in anomaly detection, malware identification, and automated defense mechanisms. Still, its standalone capabilities remain limited when confronting increasingly adaptive and state-sponsored cyber adversaries [6], [12]. Current research streams have largely explored quantum computing and AI independently, yet few comprehensive studies have investigated their combined potential in constructing robust, future-ready cybersecurity frameworks [9], [13]. This absence of integrative reviews addressing the synergy between quantum computational capacity and intelligent learning systems represents a critical gap in the literature. Closing this gap is urgent, as proactive strategies are essential to prepare for quantum-enabled threats rather than relying on reactive, short-term defenses [7].

The urgency to rethink cybersecurity strategies is underscored by the looming “Q-Day,” when quantum computers are expected to gain the capability to break conventional encryption algorithms, leaving vast amounts of sensitive information exposed [7], [14]. Preparing for this transition requires proactive investments in technologies that can withstand quantum-enabled attacks rather than relying on incremental improvements to legacy systems. Quantum computing offers a paradigm shift by enabling post-quantum cryptographic methods and quantum-enhanced threat detection, while AI provides the ability to learn, adapt, and respond dynamically to evolving attack vectors [15], [16]. The combination of these technologies has the potential to not only strengthen digital resilience but also to protect critical infrastructures such as finance, energy, and healthcare, which remain prime targets of cyber adversaries [5], [17]. Beyond technical necessity, the motivation extends to safeguarding public trust and ensuring the continuity of essential services in an increasingly interconnected world. As the economic and societal impacts of cyberattacks continue to escalate, the integration of quantum and AI-driven approaches emerges as a strategic imperative [18]. This dual focus represents a shift from reactive defense mechanisms toward proactive, adaptive, and future-proof security frameworks capable of addressing threats that exceed the limitations of classical computing.

Recent research has advanced multiple dimensions of cybersecurity by separately exploring the contributions of quantum computing and AI [19], [20]. On one side, studies have focused on post-quantum cryptographic approaches, including lattice-based, code-based, and multivariate techniques, to counteract the threat posed by Shor's algorithm and similar quantum breakthroughs [11], [21]. Other efforts have emphasized the role of quantum principles such as superposition and entanglement in developing secure communication protocols and novel encryption schemes with resilience against quantum adversaries [10], [21]. Parallel to these developments, AI has been widely deployed for real-time anomaly detection, malware identification, and adaptive intrusion prevention, with machine learning models showing strong potential in scaling threat recognition across complex environments [6], [13]. However, much of this literature remains fragmented,

focusing either on quantum-resistant algorithms or AI-driven defenses in isolation. Few studies provide an integrated analysis of how quantum computational capacity can be effectively combined with AI's adaptive intelligence to create synergistic defense mechanisms [9], [22], [23]. Moreover, while practical case studies have begun to emerge in government and enterprise systems adopting post-quantum encryption, broader discussions of ethical, regulatory, and cross-disciplinary challenges remain limited [24], [25]. This fragmented landscape underscores the necessity of a comprehensive review that bridges these domains and sets a research agenda for the quantum-AI cybersecurity paradigm.

Against this backdrop, the primary objective of this paper is to provide a comprehensive review of how quantum computing and AI can be jointly leveraged to reshape cybersecurity in the era of emerging quantum threats. Unlike existing studies that address these domains separately, this review synthesizes advances in Post-Quantum Cryptography (PQC), quantum-enhanced threat detection, secure communication protocols, and AI-driven anomaly detection into a single framework. By examining the theoretical foundations, practical applications, and future directions of these technologies, the paper seeks to highlight the unique opportunities created when quantum computational capabilities are combined with adaptive machine learning algorithms [15], [26], [27]. Furthermore, the review emphasizes the necessity of integrating ethical and regulatory considerations into technological discourse, ensuring that quantum-cybersecurity solutions are accessible, equitable, and aligned with broader societal needs [25], [28]. The scope of this paper extends across both technical and non-technical dimensions: from encryption models and Quantum Key Distribution (QKD) to governance structures and digital trust. In doing so, it aims to close the gap in the current literature and offer a forward-looking perspective that guides researchers, policymakers, and industry stakeholders in preparing for the challenges of the post-quantum era.

The main contribution of this paper is its integrated perspective on quantum computing and AI as complementary foundations for next-generation cybersecurity. Unlike studies that examine these technologies in isolation, this review emphasizes their convergence as a transformative framework for addressing threats that surpass the limits of classical defenses. It synthesizes advances in quantum-resistant cryptography, QKD, and quantum random number generation with AI-driven approaches for anomaly detection, adaptive encryption, and automated defense. In addition, the paper extends the discussion beyond technical aspects by incorporating ethical and regulatory considerations such as data privacy, accessibility, and governance. This dual focus allows for a more comprehensive understanding of how technological innovation and policy frameworks must align to ensure secure, equitable adoption. By bridging technical insights with broader societal implications, the paper provides a multidimensional contribution that supports researchers, policymakers, and practitioners in preparing for the post-quantum cybersecurity era.

Building on this foundation, the paper is structured to explore both the technical and strategic dimensions of quantum-AI cybersecurity. It first outlines the principles of quantum computing and their relevance to cryptography, followed by an examination of how AI can enhance threat detection and adaptive defense. The discussion then turns to emerging applications, including post-quantum algorithms, secure communication protocols, and hybrid quantum-AI systems. Ethical and regulatory considerations are also addressed to highlight the importance of responsible adoption. Finally, the paper identifies future research directions and practical implications for governments, industries, and academia. Together, these sections aim to provide a comprehensive view of how quantum computing and AI can jointly transform cybersecurity and ensure resilience in the digital era.

## **2 | Literature Background and Theoretical Foundations**

### **2.1 | Importance of Advanced Cyber Security**

The escalating scale and sophistication of cyber threats underscore the critical importance of developing advanced cybersecurity measures. With the rise of interconnected devices, cloud platforms, and smart infrastructures, the potential impact of cyberattacks has reached unprecedented levels, exposing critical

sectors such as finance, healthcare, and energy to systemic risks [4], [5]. Traditional protocols, once sufficient for ensuring digital protection, are increasingly susceptible to advanced intrusion techniques, making it imperative to transition toward more resilient approaches [29]. The economic and societal consequences of cyber incidents—including financial losses, reputational damage, and disruption of essential services—further emphasize the need for proactive defense mechanisms [6], [30], [31]. Within this context, emerging technologies such as AI and quantum computing provide an opportunity to reimagine cybersecurity fundamentally. AI-driven models can enhance the detection of anomalies and automate rapid responses, while quantum computing offers the possibility of cryptographic techniques that are resistant to attacks from quantum-enabled adversaries [7], [10]. Together, these technologies not only strengthen the resilience of digital systems but also contribute to the stability and trustworthiness of the broader digital ecosystem. Hence, advancing cybersecurity through the integration of quantum and AI solutions has become both a technological necessity and a strategic priority for governments, enterprises, and global institutions [32].



**Fig. 1. Importance of advanced cybersecurity.**

## 2.2 | Principles of Quantum Computing

Quantum computing applies the principles of quantum mechanics to address computational challenges that far exceed the capacity of classical systems. Unlike traditional bits that exist in binary states of 0 or 1, quantum bits, or qubits, can exist in multiple states simultaneously due to the property of superposition [33]. This ability enables quantum computers to process vast amounts of data in parallel, leading to exponential improvements in problem-solving efficiency for tasks such as cryptography, optimization, and pattern recognition. Another core principle, entanglement, allows qubits to share interdependent states, meaning the change in one qubit directly affects the other, regardless of physical distance. This phenomenon provides a foundation for highly secure communication and enhanced computational power in solving complex algorithms [9].

Additionally, quantum interference enables algorithms to manipulate probability amplitudes, amplifying correct outcomes while suppressing incorrect ones, thereby accelerating problem-solving capabilities [34]. Collectively, these properties grant quantum computing the potential to disrupt fields such as cryptography, where factoring large integers and breaking encryption protocols could be performed in a fraction of the time required by classical computers [11], [35], [36]. By harnessing superposition, entanglement, and interference, quantum computing presents unprecedented opportunities for strengthening cybersecurity, while simultaneously creating new vulnerabilities that demand proactive research and innovation [10].

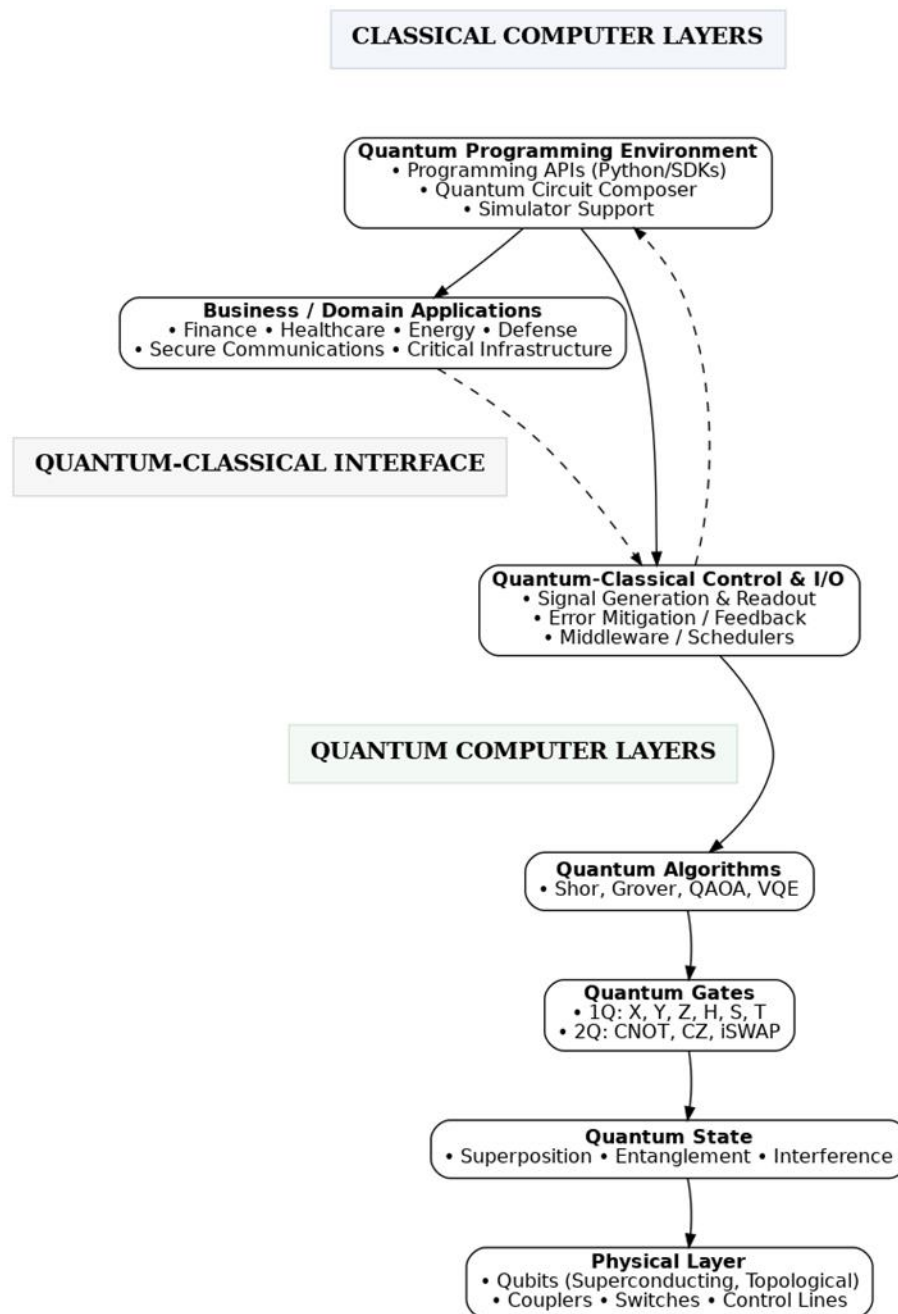


Fig. 2. Classical computer layers.

## 2.3 | Implications for Cryptography and Cyber Defense

The emergence of quantum computing poses a fundamental challenge to existing cryptographic systems, many of which depend on the difficulty of factoring large integers or solving discrete logarithm problems for their security guarantees. Algorithms such as RSA and ECC, long regarded as robust standards, could be efficiently broken by quantum algorithms such as Shor's, thereby undermining the confidentiality of sensitive data and secure communications [37]–[39]. This threat has accelerated global research efforts into PQC, including lattice-based, code-based, and multivariate encryption schemes, all designed to resist attacks from quantum-enabled adversaries [40]. Beyond cryptography, quantum computing also offers new pathways for enhancing cyber defense. Its massive parallelism allows for rapid analysis of large-scale datasets, which can significantly improve anomaly detection and vulnerability assessment [15], [41], [42]. When combined with AI, this computational power supports the development of adaptive, real-time defense mechanisms capable of countering Advanced Persistent Threats (APTs) [16]. Moreover, QKD provides a novel framework for



secure communication, where any attempt to eavesdrop can be immediately detected through disturbances in quantum states [21], [43]. These implications highlight both the vulnerabilities introduced by quantum breakthroughs and the opportunities to reimagine cybersecurity as a field shaped by quantum resilience and intelligent defense.

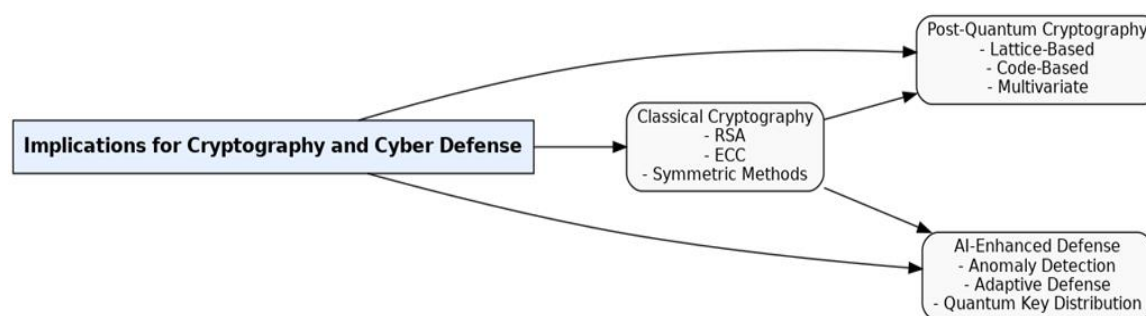


Fig. 3. Implication for cryptography and cyber defense.

## 3| Quantum Computing in Cryptography

### 3.1| Vulnerabilities of Classical Cryptography

Classical cryptographic systems, including RSA, ECC, and Diffie–Hellman key exchange, form the foundation of modern digital security. Their strength is rooted in the computational difficulty of mathematical problems such as integer factorization and discrete logarithms, which remain infeasible for classical computers to solve within practical timeframes. However, the emergence of quantum computing threatens to dismantle these assumptions. Quantum algorithms, most notably Shor’s algorithm, can efficiently solve factorization and discrete logarithm problems, thereby rendering RSA and ECC vulnerable to decryption once scalable quantum machines are realized [44]–[46]. This vulnerability implies that encrypted data secured today could be intercepted and stored for future decryption, a threat known as “harvest now, decrypt later.” Even symmetric cryptographic methods, while more resilient, are not immune; Grover’s algorithm theoretically reduces the effective security of symmetric keys by half, necessitating larger key sizes to maintain comparable protection levels [9]. The growing evidence that classical encryption methods cannot withstand quantum-enabled adversaries underscores the urgency for alternative solutions. Without a transition toward quantum-resistant protocols, sensitive information across financial systems, healthcare records, and national security communications will face unprecedented exposure [10]. These vulnerabilities form the foundation for developing post-quantum cryptographic approaches that aim to secure the digital ecosystem against the disruptive potential of quantum computing [47], [48].

### 3.2| Post-Quantum Cryptography Approaches

The vulnerabilities of classical cryptographic systems have accelerated the development of PQC, a field focused on designing algorithms resistant to quantum-based attacks. Unlike RSA or ECC, which rely on factorization and discrete logarithms, PQC methods are built upon mathematical problems that remain computationally hard even for quantum algorithms. Among these, lattice-based cryptography has emerged as the most promising due to its strong security assumptions and relatively efficient implementation. Protocols such as Kyber and NTRU are leading candidates in this domain, offering resistance against both classical and quantum adversaries [40], [49]. Code-based systems, exemplified by the McEliece cryptosystem, provide another robust option, though they often face challenges in terms of large key sizes. Multivariate polynomial cryptography and hash-based signatures also contribute to the arsenal of quantum-resistant solutions, with particular strengths in digital authentication [11]. To streamline adoption, international bodies such as the National Institute of Standards and Technology (NIST) are actively standardizing PQC algorithms, marking a critical milestone in preparing for a post-quantum era. While these approaches promise strong security, challenges remain in balancing performance, scalability, and integration into existing infrastructures [24], [50].

Nevertheless, PQC represents a proactive and necessary step to ensure the confidentiality, integrity, and availability of data in an age of quantum-enabled threats.

### 3.3 | Quantum Key Distribution

While post-quantum cryptographic algorithms aim to secure data through mathematical complexity, QKD represents a fundamentally different paradigm, leveraging the principles of Quantum mechanics to achieve theoretically unbreakable communication channels. QKD protocols, such as BB84 and E91, utilize the behavior of quantum states to generate and distribute encryption keys between parties securely. Any attempt at eavesdropping inevitably disturbs the quantum states being transmitted, thereby alerting communicators to the presence of intrusion [21]. This property, rooted in the Heisenberg uncertainty principle and quantum entanglement, provides a level of security unattainable by classical methods [43]. Unlike PQC, which relies on computational hardness, QKD ensures security by the laws of physics, making it resistant even to future advancements in quantum algorithms [51]. However, practical implementation of QKD is not without challenges. The requirement for specialized hardware, high transmission costs, and limitations in range pose significant barriers to widespread adoption [10]. Additionally, integration with existing communication infrastructures remains an ongoing research challenge. Despite these obstacles, QKD is increasingly being tested in government and enterprise networks as a complementary security measure alongside classical and PQC [52], [53]. Its promise of secure communication in a quantum era positions QKD as a cornerstone technology in the evolving landscape of cybersecurity.

### 3.4 | Artificial Intelligence Integration with Quantum Cryptography

The integration of AI with quantum cryptography represents a promising frontier in strengthening cybersecurity against increasingly adaptive threats. While quantum-resistant algorithms and QKD offer robust protection, their effectiveness can be further enhanced through AI-driven optimization and real-time management. AI, particularly machine learning models, can dynamically monitor communication channels, detect anomalies, and adapt cryptographic protocols in response to evolving attack patterns [13], [54]. For instance, AI algorithms can be employed to manage quantum keys, optimizing their distribution and renewal cycles to maintain security in highly dynamic network environments. Moreover, the combination of AI with quantum-enhanced computational capabilities offers opportunities for automating complex defense mechanisms that are impractical with classical systems alone [6]. This synergy also supports the development of intelligent intrusion detection systems that can rapidly analyze massive datasets and flag suspicious activity before it escalates into a full-scale breach. However, integrating AI with quantum cryptography also raises concerns, including the risks of adversarial attacks on AI models and the need for explainability in security-critical environments. Despite these challenges, the convergence of AI and quantum cryptography is widely regarded as a key enabler of proactive and adaptive defense strategies, providing resilience against threats that will define the post-quantum cybersecurity landscape [55].

### 3.5 | Case Studies and Practical Adoption

The transition toward quantum-resistant security is not only a theoretical endeavor but also a practical necessity being addressed by governments and enterprises worldwide. Several case studies highlight how organizations are beginning to integrate PQC into their infrastructures to prepare for the eventual advent of quantum adversaries. Government agencies have initiated pilot projects adopting lattice-based and code-based algorithms as part of their communication and data protection frameworks, providing valuable insights into deployment challenges such as interoperability, performance, and scalability [49], [56]. Similarly, enterprises in critical sectors—including finance, energy, and healthcare—are testing PQC solutions alongside traditional methods to ensure continuity of operations during the migration phase [24]. These trials underscore both the benefits and complexities of adoption, particularly with regard to balancing security with computational efficiency. In parallel, post-quantum algorithms are being incorporated into commercial software and cloud services, signaling growing momentum toward mainstream adoption. Furthermore,

international standardization efforts are providing guidelines for organizations to implement PQC within existing digital infrastructures [11]. While full-scale deployment remains in its early stages, these practical initiatives illustrate that the shift toward quantum-resistant systems is already underway, reflecting a broader recognition that preparation must precede the realization of large-scale quantum computing.

### **3.6 | Discussion**

The evolution of cryptographic systems in the context of quantum computing reveals a dual narrative of vulnerability and opportunity. On one hand, classical methods such as RSA and ECC face inevitable obsolescence under quantum algorithms like Shor's, raising immediate concerns about the long-term confidentiality of sensitive information [11]. On the other hand, the rapid progress in PQC and secure communication protocols provides promising pathways toward resilient digital infrastructures. Lattice-based and code-based schemes offer robust mathematical foundations, while QKD introduces a physics-driven security model that is fundamentally resistant to interception [7], [21]. Moreover, the integration of AI enhances the adaptability of cryptographic defenses, enabling dynamic responses to evolving threats and optimizing the deployment of quantum-resistant protocols [16]. However, practical challenges persist, including performance trade-offs, infrastructure costs, and the need for seamless interoperability with legacy systems [24], [57]. Ethical and governance issues also remain, particularly regarding equitable access to quantum security solutions across regions and industries. Overall, the discussion underscores that preparing for a quantum future requires not only technological innovation but also coordinated policy and regulatory frameworks. The convergence of PQC, QKD, and AI-driven defenses thus marks a critical transition point, shaping the foundation for resilient cybersecurity strategies in the post-quantum era.

## **4 | Quantum Computing for Threat Detection and Mitigation**

### **4.1 | Limitations of Classical Threat Detection**

Traditional threat detection systems rely heavily on classical computational models and rule-based mechanisms, which struggle to keep pace with the growing complexity of cyberattacks. While signature-based detection and heuristic approaches have historically provided reliable defenses, they are often ineffective against sophisticated techniques such as zero-day exploits, polymorphic malware, and APTs. These attacks are designed to evade conventional monitoring tools by altering their behavior or exploiting undiscovered vulnerabilities, rendering classical methods reactive rather than proactive [58]. Furthermore, the exponential growth of digital data across interconnected networks has overwhelmed the analytical capacity of conventional systems, resulting in high rates of false positives and delayed responses [6]. As cyber adversaries increasingly leverage automation and state-sponsored resources, classical systems often lack the scalability and adaptability needed to counter such persistent threats [31]. Another limitation arises from the latency of detection: by the time an anomaly is recognized, the attack has often already infiltrated critical systems, causing significant disruption or data loss. These challenges highlight the inadequacy of traditional detection models in addressing the dynamic and large-scale nature of modern cyber threats [47], [59]. Consequently, there is a pressing need for disruptive approaches, such as quantum-enhanced data processing and AI integration, to strengthen detection and mitigation strategies in real time.

### **4.2 | Quantum-Enhanced Data Processing**

One of the most promising applications of quantum computing in cybersecurity lies in its ability to accelerate data processing for threat detection. Unlike classical computers, which analyze data sequentially, quantum systems exploit superposition and entanglement to perform parallel computations across vast datasets. This capability allows for rapid identification of anomalies and attack patterns that would overwhelm traditional systems [15]. For example, intrusion detection systems equipped with quantum algorithms could process network traffic in real time, distinguishing malicious behavior from normal activity with far greater accuracy and speed. Similarly, malware analysis could benefit from quantum parallelism, enabling the simultaneous



evaluation of multiple variants of malicious code to detect subtle modifications designed to evade classical defenses [10]. Quantum computing also enhances the scalability of defensive systems by reducing the computational overhead typically associated with large-scale monitoring tasks [9], [60]. These improvements are especially valuable in environments where latency can determine whether an intrusion is neutralized before it causes damage. While practical deployment is currently constrained by the limitations of Noisy Intermediate-Scale Quantum (NISQ) devices, ongoing research suggests that even hybrid quantum-classical systems can offer measurable improvements in detection speed and accuracy. By leveraging quantum-enhanced data processing, organizations can move toward proactive defense mechanisms that operate at the speed and scale of modern cyber threats.

### 4.3 | Integration with Artificial Intelligence

The convergence of quantum computing and AI presents a transformative opportunity for strengthening cyber defense. While quantum systems provide unparalleled computational capacity, AI contributes adaptability and learning capabilities that are essential for managing evolving threats. Quantum Machine Learning (QML) models, for instance, have the potential to accelerate the training and inference processes of anomaly detection systems, enabling faster recognition of sophisticated attack vectors across dynamic environments [6]. By leveraging quantum-enhanced algorithms, AI can analyze high-dimensional data more efficiently, identifying patterns and correlations that remain hidden to classical approaches [13]. This integration also supports proactive defense: AI-driven decision-making can adapt quantum-enhanced cryptographic and detection protocols in real time, strengthening resilience against zero-day attacks and APTs. Furthermore, hybrid quantum-AI systems can automate vulnerability scanning, optimize resource allocation, and deploy predictive models that anticipate attacker behavior [10]. Despite these advantages, challenges remain, particularly concerning the interpretability of AI models and the technical limitations of current quantum hardware. Adversarial attacks on AI systems also raise concerns about trust and reliability in critical cybersecurity operations [61]. Nonetheless, the integration of quantum computing with AI represents a pivotal step toward adaptive, intelligent, and future-proof defense architectures, shifting cybersecurity strategies from reactive monitoring to dynamic and predictive protection.

### 4.4 | Optimization in Cyber Defense

Beyond accelerating data analysis, quantum computing also offers powerful capabilities in solving optimization problems that are central to cybersecurity. Classical defense systems often struggle with resource allocation, network optimization, and vulnerability management due to the combinatorial complexity of these tasks. Quantum algorithms, particularly those designed for combinatorial optimization, can evaluate multiple configurations simultaneously, providing efficient solutions to problems that classical systems can only approximate [9]. For instance, in patch management, quantum-enhanced optimization could prioritize vulnerabilities based on risk severity and potential impact, ensuring that critical systems are protected first. Similarly, in large-scale network defense, quantum algorithms can optimize traffic routing to minimize exposure to attack vectors while maintaining performance [15]. These methods can also improve scheduling in Security Operations Centers (SOCs), where limited analyst resources must be strategically allocated to address the most pressing threats. Moreover, hybrid quantum-classical models offer practical pathways for applying these techniques in the NISQ era, balancing theoretical potential with current hardware limitations [10]. By introducing greater efficiency and intelligence into core defensive operations, quantum optimization not only strengthens resilience but also reduces the costs and inefficiencies associated with conventional approaches. This positions optimization as a key area where quantum computing can deliver immediate and tangible benefits for cybersecurity.

## 4.5 | Conceptual Framework for Threat Mitigation

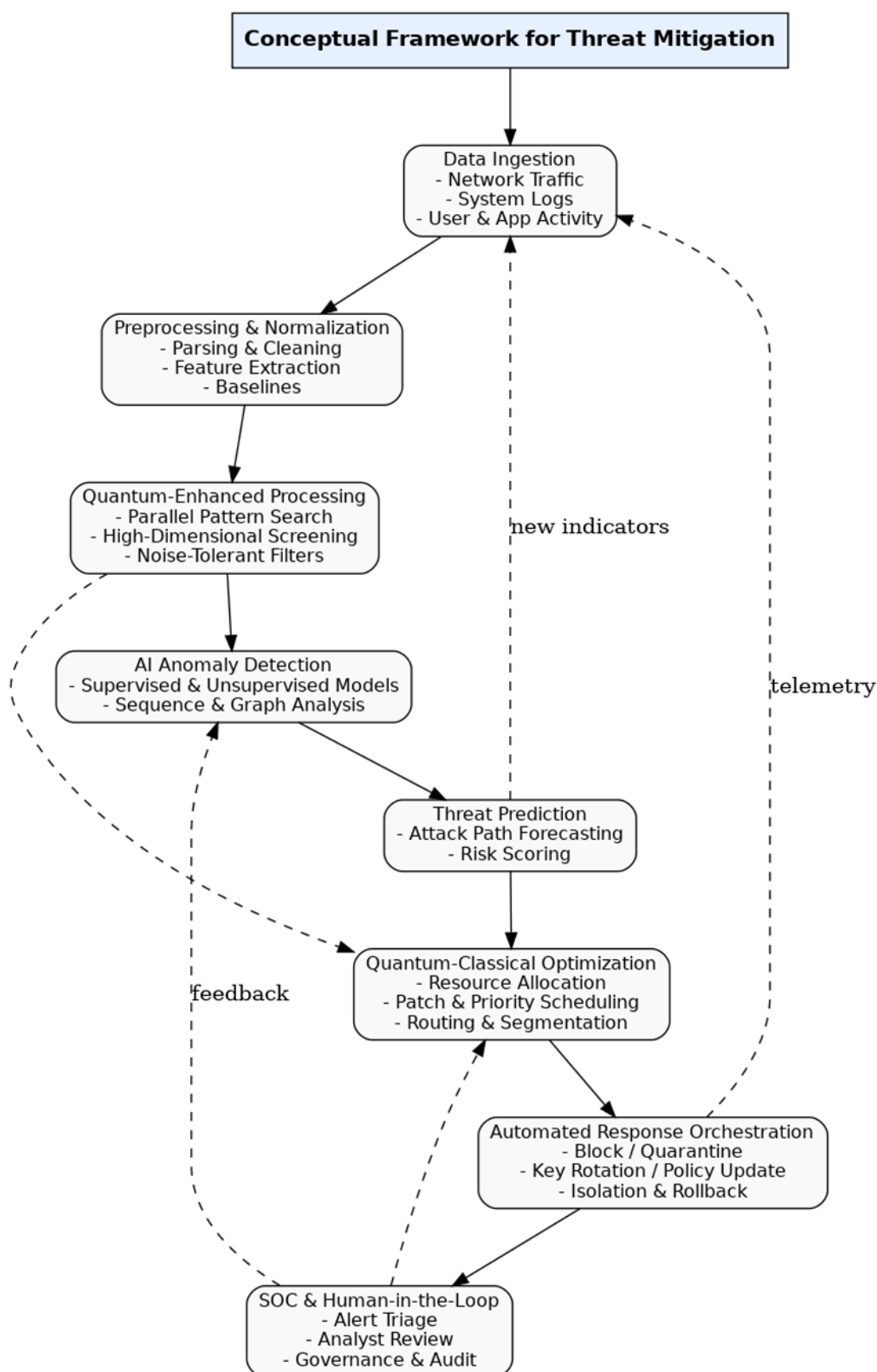


Fig. 4. Conceptual Framework.

## 4.6 | Challenges and Direction

While the integration of quantum computing into cybersecurity offers transformative opportunities, several challenges limit its near-term adoption. Foremost among these are the technological constraints of NISQ devices, which suffer from instability, limited qubit counts, and high error rates [10]. These limitations restrict the scalability of quantum algorithms and make their deployment in real-world security environments difficult. Cost is another concern, as the specialized infrastructure required for quantum systems remains prohibitively expensive for widespread organizational use [11], [24]. Additionally, interoperability between classical, quantum, and AI-based defense systems poses a critical barrier, demanding hybrid architectures capable of seamless integration. Ethical and governance issues also complicate adoption; unequal access to quantum security solutions risks deepening global disparities in cybersecurity resilience [25]. Looking ahead, research is increasingly focused on developing noise-resistant algorithms, hybrid quantum–classical models, and error-correction strategies to improve performance in the NISQ era [9]. Parallel efforts in standardization and regulatory frameworks are essential to ensure responsible and equitable deployment. Ultimately, the future of quantum-enabled threat mitigation will depend not only on overcoming technical barriers but also on fostering interdisciplinary collaboration among scientists, policymakers, and industry leaders. These steps are critical to realizing the promise of proactive, scalable, and trustworthy cybersecurity in the post-quantum era.

## 5 | Quantum-Enhanced Security Protocols

### 5.1 | Quantum Random Number Generators

Randomness plays a central role in cryptographic systems, serving as the foundation for secure key generation, encryption, and authentication processes. Classical random number generators, however, often rely on deterministic algorithms or pseudo-random processes that may be predictable or vulnerable to sophisticated attacks. Quantum Random Number Generators (QRNGs) address this limitation by exploiting inherent quantum mechanical phenomena—such as photon arrival times, vacuum fluctuations, or quantum noise—to produce true randomness that cannot be replicated or anticipated [21]. Unlike classical approaches, QRNG outputs are non-deterministic and verifiable, offering a significant boost in security for cryptographic applications. They are particularly valuable in the context of quantum-resistant and hybrid encryption protocols, where ensuring unpredictability is critical to resisting brute-force and side-channel attacks [10]. Moreover, QRNGs can be integrated into existing infrastructures through hardware devices or cloud-based services, making them more accessible to enterprises seeking enhanced security. Despite their promise, challenges remain in terms of scalability, cost, and standardization, as widespread deployment requires ensuring both affordability and compatibility with current systems [24]. Nevertheless, QRNGs represent a key building block of quantum-enhanced security, reinforcing the unpredictability and resilience of encryption mechanisms in anticipation of quantum-era threats.

### 5.2 | Secure Communication Protocol

Secure communication lies at the heart of cybersecurity, and quantum technologies are redefining how information can be transmitted with resilience against advanced adversaries. Beyond traditional encryption schemes, quantum-secure communication protocols leverage principles such as superposition and entanglement to establish channels that are inherently resistant to eavesdropping. The most notable example is QKD, which enables two parties to exchange cryptographic keys while guaranteeing that any interception attempt will disturb the quantum states and thus be immediately detectable [21], [43]. This physical guarantee of security distinguishes QKD from classical key exchange methods, which depend solely on computational hardness assumptions. In addition to QKD, protocols such as quantum teleportation and entanglement-based communication are being investigated to further strengthen confidentiality and integrity [10] further. While experimental demonstrations have validated the feasibility of secure quantum channels across fiber-optic and satellite networks, real-world adoption remains limited by issues of cost, distance, and infrastructure readiness [62]. Hybrid models that combine QKD with PQC are emerging as practical solutions, bridging the gap

between theoretical promise and operational feasibility [24]. These protocols represent a paradigm shift in communication security, providing a robust foundation for safeguarding sensitive data in financial, governmental, and critical infrastructure sectors against both classical and quantum-enabled adversaries.

### 5.3 | Hybrid Quantum–Classical Security Models

Given the limitations of current quantum hardware, fully quantum security infrastructures remain impractical in the near term. As a result, hybrid quantum–classical security models have emerged as a transitional strategy, integrating quantum capabilities with established classical frameworks. These models combine the scalability and maturity of classical systems with the unique advantages of quantum techniques such as QKD, QRNGs, and post-quantum cryptographic algorithms [10]. For example, a hybrid network may use classical encryption methods for data transmission while relying on QKD for secure key exchange, thereby strengthening confidentiality without requiring a complete overhaul of existing infrastructure [21]. Similarly, QRNGs can be embedded into classical systems to enhance key unpredictability, reinforcing resilience against brute-force and side-channel attacks [24]. Hybrid approaches also enable organizations to adopt quantum technologies gradually, mitigating costs and compatibility challenges while preparing for long-term quantum readiness [40], [63]. However, these models raise concerns about interoperability, performance optimization, and potential new vulnerabilities introduced at the intersection of classical and quantum systems. Despite these challenges, hybrid security models represent a practical and incremental pathway toward the post-quantum era, ensuring that organizations can benefit from quantum-enhanced protection while maintaining continuity with established cybersecurity practices.

### 5.4 | Ethical and Governance Considerations

The adoption of quantum-enhanced security protocols extends beyond technical innovation and raises significant ethical and governance challenges. While quantum technologies promise unprecedented levels of protection, their uneven development and distribution risk widening the digital divide between nations and organizations with advanced resources and those lacking access [25]. Such disparities could create asymmetries in global security, leaving vulnerable regions exposed to threats from adversaries equipped with quantum capabilities. Ethical concerns also emerge around privacy, as the integration of quantum-secure communication networks may enable unprecedented monitoring and control if misused by state or corporate actors [24]. Governance frameworks are therefore critical to ensure that quantum security is deployed responsibly, transparently, and equitably. International collaboration is particularly important, as cyber threats transcend borders, demanding harmonized standards and cooperative security protocols [22]. Furthermore, the integration of AI with quantum systems introduces accountability challenges, especially when automated defense decisions affect sensitive data or critical services [6]. Policymakers and industry leaders must therefore balance technological advancement with ethical safeguards, ensuring that trust, fairness, and inclusivity remain central to quantum adoption. Establishing robust regulatory and oversight mechanisms will be essential in shaping the responsible trajectory of quantum-enhanced cybersecurity.

## 6 | Conclusion

The advent of quantum computing represents both a profound challenge and an unprecedented opportunity for the future of cybersecurity. Classical cryptographic systems, long relied upon to safeguard digital infrastructures, face obsolescence under the disruptive power of quantum algorithms such as Shor’s and Grover’s. At the same time, the convergence of PQC, QKD, and AI provides a foundation for designing resilient defenses capable of withstanding even the most advanced adversaries. This review has highlighted the vulnerabilities of existing systems, explored the development of quantum-resistant algorithms, and examined emerging solutions such as QRNGs, hybrid quantum–classical models, and AI-driven anomaly detection. It has also emphasized the importance of optimization, proactive threat mitigation, and secure communication protocols in shaping next-generation defenses. Beyond technological advancements, the paper has underscored the ethical and governance dimensions of adopting quantum-enhanced security.

Equitable access, transparency, and international collaboration are essential to ensure that these innovations benefit global security rather than exacerbate existing inequalities. Looking ahead, success in navigating the quantum transition will depend on interdisciplinary collaboration between researchers, policymakers, and industry leaders. By aligning technical innovation with ethical responsibility, the cybersecurity community can move toward a future that is not only secure but also resilient and trustworthy. In doing so, quantum computing and AI may transform cybersecurity from a reactive practice into a proactive, adaptive, and enduring defense paradigm for the digital era.

## References

- [1] Butler, P., Kelley, J., Ellis, J., & Olatunbosun, S. (2024). Cybersecurity threats: An analysis of the rise and impacts of state sponsored cyber attacks. *World congress in computer science, computer engineering & applied computing* (pp. 187–194). Springer Nature Switzerland. [https://doi.org/10.1007/978-3-031-86644-9\\_14](https://doi.org/10.1007/978-3-031-86644-9_14)
- [2] Raihan, A., Bala, S., Akther, A., Ridwan, M., Eleais, M., & Chakma, P. (2024). Advancing environmental sustainability in the G-7: The impact of the digital economy, technological innovation, and financial accessibility using panel ARDL approach. *Journal of economy and technology*. <https://doi.org/10.1016/j.ject.2024.06.001>
- [3] Rahman, J., Rahman, H., Islam, N., Tanchangya, T., Ridwan, M., & Ali, M. (2025). Regulatory landscape of blockchain assets: Analyzing the drivers of NFT and cryptocurrency regulation. *BenchCouncil transactions on benchmarks, standards and evaluations*, 100214. <https://doi.org/10.1016/j.tbench.2025.100214>
- [4] Blogs, M. C. (2024). *Prioritizing security above all else*. <https://blogs.microsoft.com/blog/2024/05/03/prioritizing-security-above-all-else>
- [5] EBR, E. (2024). *Securing critical infrastructure: Protecting vital systems from cyber threats - The European business review*. <https://www.europeanbusinessreview.com/securing-critical-infrastructure-protecting-vitalsystems-from-cyber-threats>
- [6] Aurangzeb, M., Wang, Y., Iqbal, S., Naveed, A., Ahmed, Z., Alenezi, M., & Shouran, M. (2024). Enhancing cybersecurity in smart grids: Deep black box adversarial attacks and quantum voting ensemble models for blockchain privacy-preserving storage. *Energy reports*, 11, 2493–2515. <https://doi.org/10.1016/j.egyr.2024.02.010>
- [7] Pereira, D. (2024). Quantum day (aka “Q-Day”) is a gray rhino stridently galloping straight at your organization. <https://www.oodalooop.com/archive/2024/04/04/quantum-day-aka-q-day-is-a-gray-rhino-stridentlygalloping>
- [8] Raihan, A., Rahman, S. M., Ridwan, M., & Sarker, T. (2025). FinTech adoption and its influence on sustainable mineral resource management in the united states. *Resources*, 14(6), 101. <https://doi.org/10.3390/resources14060101>
- [9] Hoefler, T., Häner, T., & Troyer, M. (2023). Disentangling hype from practicality: On realistically achieving quantum advantage. *Communications of the acm*, 66(5), 82–87. <https://dl.acm.org/doi/fullHtml/10.1145/3571725>
- [10] Rehman, M. U. (2024). Quantum-enhanced chaotic image encryption: Strengthening digital data security with 1-D sine-based chaotic maps and quantum coding. *Journal of king saud university-computer and information sciences*, 36(3), 101980. <https://doi.org/10.1016/j.jksuci.2024.101980>
- [11] Boutin, C. (2023). NIST to standardize encryption algorithms that can resist attack by quantum computers. *NIST news*. <https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers>
- [12] Ridwan, M., Urbee, A. J., Voumik, L. C., Das, M. K., Rashid, M., & Esquivias, M. A. (2024). Investigating the environmental Kuznets curve hypothesis with urbanization, industrialization, and service sector for six south Asian countries: Fresh evidence from driscoll kraay standard error. *Research in globalization*, 8, 100223. <https://doi.org/10.1016/j.resglo.2024.100223>
- [13] Gonaygunta, H., Nadella, G. S., Pawar, P. P., & Kumar, D. (2024). Enhancing cybersecurity: The development of a flexible deep learning model for enhanced anomaly detection. *2024 systems and information engineering design symposium (SIEDS)* (pp. 79–84). IEEE. <https://doi.org/10.1109/SIEDS61124.2024.10534661>
- [14] Can, M. (2024). *Artificial intelligence as a resource: An appraisal of china's mobilization and extraction strategies*.
- [15] Baker, B. (2024). *Quantum A.I. model improves early cyber threat detection*. <https://aibusiness.com/quantum-computing/quantum-ai-model-improves-early-cyber-threat-detection>
- [16] Gonaygunta, H., Nadella, G. S., Pawar, P. P., & Kumar, D. (2024). Study on empowering cyber security by using adaptive machine learning methods. *2024 systems and information engineering design symposium (SIEDS)* (pp. 166–171). IEEE. <https://doi.org/10.1109/SIEDS61124.2024.10534694>



- [17] Akther, A., Tahrim, F., Voumik, L. C., Esquivias, M. A., & Pattak, D. C. (2025). Municipal solid waste dynamics: Economic, environmental, and technological determinants in Europe. *Cleaner engineering and technology*, 24, 100877. <https://doi.org/10.1016/j.clet.2024.100877>
- [18] Boretti, A. (2024). Technical, economic, and societal risks in the progress of artificial intelligence driven quantum technologies. *Discover artificial intelligence*, 4(1), 67. <https://doi.org/10.1007/s44163-024-00171-y>
- [19] Ahmad, S., Raihan, A., & Ridwan, M. (2024). Role of economy, technology, and renewable energy toward carbon neutrality in China. *Journal of economy and technology*, 2, 138–154. <https://doi.org/10.1016/j.ject.2024.04.008>
- [20] Mozumder, M. A. S., Nguyen, T. N., Devi, S., Arif, M., Ahmed, M. P., Ahmed, E., Uddin, A. (2024). Enhancing customer satisfaction analysis using advanced machine learning techniques in fintech industry. *Journal of computer science and technology studies*, 6(3), 35–41. <https://doi.org/10.32996/jcsts>
- [21] Renner, R., & Wolf, R. (2023). Quantum advantage in cryptography. *AIAA journal*, 61(5), 1895–1910. <https://doi.org/10.2514/1.J062267>
- [22] Rahman, M. H., Das, A. C., Shak, M. S., Uddin, M. K., Alam, M. I., Anjum, N., ... , & Alam, M. (2024). Transforming customer retention in fintech industry through predictive analytics and machine learning. *The American journal of engineering and technology*, 6(10), 150–163. <https://doi.org/10.5281/zenodo.14008362>
- [23] Ridwan, M. (2023). Unveiling the powerhouse: Exploring the dynamic relationship between globalization, urbanization, and economic growth in Bangladesh through an innovative ARDL approach. *ASIAN journal of economics and business management*, 283\_291. <https://doi.org/10.53402/ajebm.v2i2.352>
- [24] von Nethen, N., Wiesmaier, A., Weissmann, O., & Alnahawi, N. (2023). PMMP\_PQC migration management process. *Computer science > cryptography and security*, 1(4), 17. <https://doi.org/10.48550/arXiv.2301.04491>
- [25] Scanlon, T. (2024). Cybersecurity of quantum computing: A new frontier. *Apr*, 10, 22023. <https://doi.org/10.58012/rzmt-m258>
- [26] Ridzuan, A. R., Rahman, N. H. A., Singh, K. S. J., Borhan, H., Ridwan, M., Voumik, L. C., Ali, M. (2023). Assessing the impact of technology advancement and foreign direct investment on energy utilization in malaysia: an empirical exploration with boundary estimation. *International conference on business and technology* (pp. 1–12). Springer Nature Switzerland. [https://doi.org/10.1007/978-3-031-55911-2\\_1%0A%0A](https://doi.org/10.1007/978-3-031-55911-2_1%0A%0A)
- [27] Arif, M., Hasan, M., Al Shiam, S. A., Ahmed, M. P., Tusher, M. I., Hossan, M. Z., ... , & Imam, T. (2024). Predicting customer sentiment in social media interactions: Analyzing amazon help Twitter conversations using machine learning. *International journal of advanced science computing and engineering*, 6(2), 52–56. <https://doi.org/10.62527/ijasce.6.2.211>
- [28] Urbee, A. J., Ridwan, M., & Raihan, A. (2024). Exploring educational attainment among individuals with physical disabilities: A case study in Bangladesh. *Journal of integrated social sciences and humanities*. <https://doi.org/10.62836/jissh.v1i1.181>
- [29] Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, 23(15), 6666. <https://doi.org/10.3390/s23156666>
- [30] Hossain, M. N., Anjum, N., Alam, M., Rahman, M. H., Taluckder, M. S., Al Bony, M. N. V., ... , & Jui, A. H. (2024). Performance of machine learning algorithms for lung cancer prediction: A comparative study. *International journal of medical science and public health research*, 5(11), 41–55. <https://doi.org/10.37547/ijmsphr/Volume05Issue11-05>
- [31] Onwe, J. C., Ridzuan, A. R., Uche, E., Ray, S., Ridwan, M., & Razi, U. (2024). Greening Japan: Harnessing energy efficiency and waste reduction for environmental progress. *Sustainable futures*, 8, 100302. <https://doi.org/10.1016/j.sftr.2024.100302>
- [32] Radanliev, P. (2025). Cyber diplomacy: Defining the opportunities for cybersecurity and risks from artificial intelligence, IoT, Blockchains, and quantum computing. *Journal of cyber security technology*, 9(1), 28–78. <https://doi.org/10.1080/23742917.2024.2312671>
- [33] Conversation, T. (2023). *A computer scientist explains how quantum advantage could change the world*. <https://www.fastcompany.com/90987214/a-computer-scientist-explains-how-quantum-advantage-could-change-the-world>
- [34] Nourbakhsh, A., Jones, M. N., Kristjuhan, K., Carberry, D., Karon, J., Beenfeldt, C., Mansouri, S. S. (2022). *quantum computing: Fundamentals, trends and perspectives for chemical and biochemical engineers*. <https://doi.org/10.48550/arXiv.2201.02823>

- [35] Sweet, M. M. R., Arif, M., Uddin, A., Sharif, K. S., Tusher, M. I., Devi, S. (2024). Credit risk assessment using statistical and machine learning: Basic methodology and risk modeling applications. *International journal on computational engineering*, 1(3), 62–67. <https://doi.org/10.62527/comien.1.3.21>
- [36] Ridwan, M., Akther, A., Tamim, M. A., Ridzuan, A. R., Esquivias, M. A., & Wibowo, W. (2024). Environmental health in BIMSTEC: The roles of forestry, urbanization, and financial access using LCC theory, DKSE, and quantile regression. *Discover sustainability*, 5(1), 429. <https://doi.org/10.1007/s43621-024-00679-4%0A%0A>
- [37] Sahu, S. K., & Mazumdar, K. (2024). State-of-the-art analysis of quantum cryptography: Applications and future prospects. *Frontiers in physics*, 12, 1456491. <https://doi.org/10.3389/fphy.2024.1456491>
- [38] Shak, M. S., Uddin, A., Rahman, M. H., Anjum, N., Al Bony, M. N. V., Alam, M., ... , & Pervin, T. (2024). Innovative machine learning approaches to foster financial inclusion in microfinance. *International interdisciplinary business economics advancement journal*, 5(11), 6–20. <https://doi.org/10.55640/business/volume05issue11-02>
- [39] Orthi, S. M., Rahman, M. H., Siddiqua, K. B., Uddin, M., Hossain, S., Al Mamun, A., & Khan, M. N. (2025). Federated learning with privacy-preserving big data analytics for distributed healthcare systems. *Journal of computer science and technology studies*, 7(8), 269–281. <https://doi.org/10.32996/jcsts.2025.7.8.31>
- [40] Yalamuri, G., Honnavalli, P., & Eswaran, S. (2022). A review of the present cryptographic arsenal to deal with post-quantum threats. *Procedia computer science*, 215, 834–845. <https://doi.org/10.1016/j.procs.2022.12.086>
- [41] Rahman, M., Al Amin, M., Hasan, R., Hossain, S. M. T., Rahman, M. H., & Rashed, R. A. M. (2025). A Predictive AI framework for cardiovascular disease screening in the us: Integrating EHR data with machine and deep learning models. *British journal of nursing studies*, 5(2), 40–48. <https://doi.org/10.32996/bjns.2025.5.2.5>
- [42] Ridwan, M., Akther, A., Dhar, B. K., Roshid, M. M., Mahjabin, T., Bala, S., & Hossain, H. (2025). Advancing circular economy for climate change mitigation and sustainable development in the nordic region. *Sustainable development*, 1\_20. <https://doi.org/10.1002/sd.3563>
- [43] Jain, N., Chin, H.-M., Hajomer, A. A. E., Null, D., Larfort, H., Nysom, N. L., Gehring, T. (2024). Future proofing network encryption technology with continuous-variable quantum key distribution. *Optics express*, 32(24), 43607–43620. <https://doi.org/10.48550/arXiv.2402.18881>
- [44] Rahman, M. D. H., Rahaman, M., Arafat, Y., Rahat, S. K. R. U. I., Hasan, R., Rimon, S. M. T. H., & Dipa, S. A. (2025). Artificial intelligence for chronic kidney disease risk stratification in the USA: Ensemble vs. deep learning methods. *British journal of nursing studies*, 5(2), 20–32. <https://doi.org/10.32996/bjns.2025.5.2.3>
- [45] Rahat, S. K. R. U. I., RAHMAN, M. D. H., Arafat, Y., Rahaman, M., Hasan, M. M., & Al Amin, M. (2025). Advancing diabetic retinopathy detection with AI and deep learning: Opportunities, limitations, and clinical barriers. *British journal of nursing studies*, 5(2), 1–13. <https://doi.org/10.32996/bjns.2025.5.2.1>
- [46] Akash, M. A., Riaz, M. H., Uddin, M. N., Ridwan, M., Akinpelu, A. A., & Akter, R. (2025). Analyzing the drivers of ecological footprint toward sustainability in BRICS+. *Environment, innovation and management*, 1, 2550017. <https://doi.org/10.1142/S3060901125500176>
- [47] Rahman, M. H., Anwar, M. M., & Hossain, F. (2025). AI-driven big data and business analytics: Advancing healthcare, precision medicine, supply chain resilience, energy innovation and economic competitiveness. *Journal of medical and health studies*, 6(3), 205–215. <https://doi.org/10.32996/jmhs.2025.6.3.30>
- [48] Rahman, M. H., Dipa, S. A., Hasan, K., & Hasan, M. M. (2025). Health at risk: Respiratory, cardiovascular, and neurological impacts of air pollution. *Innovations in environmental economics*, 1(1), 56–69. <https://doi.org/10.48313/iee.v1i1.41>
- [49] Nguyen, H., Huda, S., Nogami, Y., & Nguyen, T. T. (2025). Security in post-quantum era: A comprehensive survey on lattice-based algorithms. *IEEE access*, 13, 89003\_89024. <https://doi.org/10.1109/ACCESS.2025.3571307>
- [50] Rahman, M. H., Hossin, M. E., Hossain, M. J., Uddin, S. M. M., Faruk, M. I., Anwar, M. M., & Hossain, F. (2024). Harnessing big data and predictive analytics for early detection and cost optimization in cancer care. *Journal of computer science and technology studies*, 6(5), 278–293. <https://doi.org/10.32996/>
- [51] Fathalla, E., & Azab, M. (2024). Beyond classical cryptography: A systematic review of post-quantum hash-based signature schemes, security, and optimizations. *IEEE access*, 12, 175969\_175987. <https://doi.org/10.1109/ACCESS.2024.3485602>
- [52] Uddin, M. K., Akter, S., Das, P., Anjum, N., Akter, S., Alam, M., ... , & Pervin, T. (2024). Machine learning-based early detection of kidney disease: A comparative study of prediction models and performance evaluation, 5(12), 58\_75. <https://doi.org/10.37547/ijmsphr/Volume05Issue12-05>
- [53] Hasan, M. M., Riaz, M. H., Ahmed, Z., Islam, S., Uddin, M. S., Roshid, M. M., Atasoy, F. G. (2025). Decarbonizing Bangladesh: The roles of technological innovation, energy transition, and urban-industrial

- dynamics in greenhouse gas emissions. *Environment, innovation and management*, 1, 2550019. <https://doi.org/10.1142/S306090112550019X>
- [54] Gharbi, I., Rahman, M. H., Muryani, M., Esquivias, M. A., & Ridwan, M. (2025). Exploring the influence of financial development, renewable energy, and tourism on environmental sustainability in Tunisia. *Discover sustainability*, 6(1), 127. <https://doi.org/10.1007/s43621-025-00896-5%0A%0A>
- [55] Campbell, L. (2025). Post-quantum AI-based cryptographic methods for future-ready cybersecurity Infrastructure. <https://www.researchgate.net/publication/393917890>
- [56] Raihan, A., Rahman, S. M., Sarker, T., Ridwan, M., Sahoo, M., Dhar, B. K., Bari, A. B. M. M. (2025). Tourism-energy-economy-environment nexus toward sustainable and green development in malaysia. *Innovation and green development*, 4(4), 100257. <https://doi.org/10.1016/j.igd.2025.100257>
- [57] Raihan, A., Ridwan, M., Sarker, T., Atasoy, F. G., Zimon, G., Bari, A. B. M. M., Mohajan, B. (2025). The influence of different environmental factors toward Vietnam's net-zero emissions goal. *Innovation and green development*, 4(3), 100229. <https://doi.org/10.1016/j.igd.2025.100229>
- [58] Com, C. (2023). *Cyber security assessment services*. *Cybersecop*. <https://cybersecop.com/cybersecurity-assessmentservices>
- [59] Voumik, L. C., Ridwan, M., Rahman, M. H., & Raihan, A. (2023). An investigation into the primary causes of carbon dioxide releases in Kenya: Does renewable energy matter to reduce carbon emission? *Renewable energy focus*, 47, 100491. <https://doi.org/10.1016/j.ref.2023.100491>
- [60] Kurniawati, T., Rahmizal, M., Ridwan, M., Aspy, N. N., Mahjabin, T., Eleais, M., & Ridzuan, A. R. (2025). Reassessing the load capacity curve hypothesis in ASEAN-5: Exploring energy intensity, trade, and financial inclusion with advanced econometric techniques. *International journal of energy economics and policy*, 15. <https://doi.org/10.32479/ijeeep.17328>
- [61] Chen, T., Liu, J., Xiang, Y., Niu, W., Tong, E., & Han, Z. (2019). Adversarial attack and defense in reinforcement learning-from AI security view. *Cybersecurity*, 2(1), 11. <https://doi.org/10.1186/s42400-019-0027-x%0A%0A>
- [62] Raihan, A., Hasan, M. A., Voumik, L. C., Pattak, D. C., Akter, S., & Ridwan, M. (2024). Sustainability in Vietnam: Examining economic growth, energy, innovation, agriculture, and forests' impact on CO2 emissions. *World development sustainability*, 4, 100164. <https://doi.org/10.1016/j.wds.2024.100164>
- [63] Urbee, A. J., Hasan, M. A., Ridwan, M., & Dewan, M. F. (2025). Adaptation and resilience in the face of climate-induced migration: Exploring coping strategies in the urban economy of barishal metropolitan city. *Environment, innovation and management*, 1, 2550005. <https://doi.org/10.1142/S306090112550005X>