International Journal of Scientific Research in Engineering and Management (IJSREM)
Special Edition - Volume 09 NCFT -2025 SJIF Rating: 8.586 ISSN: 2582-3930

Evaluating the Impact of Quantum Algorithms on Modern Cybersecurity Mechanisms

1st Mallu Shiva Rama Krishna
School of Computer Science and Engineering
VIT-AP University
Amaravati, A.P., India.
mallu.22phd7084@vitap.ac.in
https://orcid.org/0009-0007-8950-0288

2nd Patwari KrishnaRao
Computer Science and Engineering
Geethanjali College of Engineering and Technology (Autonomous)
Hyderabad, Telangana, India.
pkrishnarao.cse@gcet.edu.in

3rd Manumula Srinubabu
Department of ECE
Aditya University
Kakinada, A.P., India.
msrinubabu37@gmail.com
https://orcid.org/0009-0004-9193-6396

***Abstract*—The emergence of quantum computing represents a fundamental challenge to contemporary cryptographic infrastructures, mandating immediate adoption of quantum-resistant cryptographic standards to ensure long-term security. This paper analyzes how Shor's algorithm renders RSA , ECC vulnerable by solving integer factorization and discrete alogarithm problems in polynomial time, while Grover's algorithm weakens symmetric encryption through quadratic speedup attacks. Through comprehensive cryptanalysis, we evaluate the vulnerabilities of current public-key infrastructures, symmetric ciphers, and hash functions against quantum threats. Our research systematically examines post-quantum cryptographic candidates, including lattice-based, hash-based, and multivariate polynomial schemes under NIST standardization, assessing their security guarantees and implementation challenges. Furthermore, we investigate the broader implications for secure communications, blockchain networks, and authentication protocols in a post-quantum world. Based on our findings, we propose a practical transition framework featuring hybrid cryptographic systems, protocol enhancements, and policy updates to facilitate seamless migration. This work provides critical insights and actionable strategies for securing digital infrastructure against quantum threats while maintaining operational efficiency during the transition period.**

***Index Terms*—Cryptographic vulnerability, Grover's algorithm, Post-quantum cryptography, Quantum computing, Quantum key distribution, Shor's algorithm, Cybersecurity**

I. Introduction

The accelerated development of quantum computing presents a dual impact on cybersecurity, simultaneously introducing transformative computational capabilities and unprecedented vulnerabilities to existing cryptographic infrastructures. Quantum computing systems offer transformative potential for solving computationally intractable problems, yet simultaneously threaten the foundational security assumptions of modern cryptography. Current cryptographic standards including RSA, ECC, and symmetric-key encryption derive their security from mathematical problems whose computational complexity may be effectively nullified by quantum algorithms. Specifically, public key cryptosystems relying on integer factorization , elliptic curve discrete logarithms become vulnerable to polynomial-time attacks to Shor's algorithm, while Grover's algorithm provides quadratic acceleration against symmetric key constructions.The growing accessibility of quantum technologies necessitates a thorough evaluation of their implications on modern cybersecurity infrastructure.

Shor'sb, Grover's algorithms underscore quantum computing's threat to modern security. Shor's algorithm efficiently factors large integers, computes discrete logarithms, jeopardizing RSA , ECC encryption. Grover's algorithm speeds up brute-force attacks on symmetric ciphers, reducing their effectiveness. Both highlight vulnerabilities in current cryptographic systems, necessitating quantum-resistant solutions, offering a quadratic speedup in the process. These capabilities threaten data confidentiality, authentication mechanisms, and the integrity of secure communication protocols. As quantum hardware continues to mature, transitioning to quantum-resilient cryptographic methods is no longer optional it is imperative.

This paper aims to assess the scope of quantum algorithms' impact on widely adopted cybersecurity mechanisms. By analyzing algorithmic vulnerabilities, simulating quantum attacks, and surveying post-quantum cryptographic solutions, we offer a comprehensive understanding of the challenges ahead. Additionally, we evaluate the readiness of emerging standards proposed by institutions such as NIST, and discuss strategic considerations for implementing quantum-safe systems. Our study serves as a timely guide for security professionals, researchers, and policymakers navigating the evolving landscape of post-quantum cybersecurity.

II. Literature Review

This research Evalutes the impact of quantum computing on cybersecurity in smart cities, with a specific focus on mitigating zero-day attacks. It introduces a defense framework that integrates quantum resilient cryptography, The framework employs AI-driven anomaly detection , hybrid quantum classical simulations. It integrates lattice based encryption for security and machine learning models for enhanced threat analysis , including LSTM , CNN, to achieve high detection accuracy , minimize false positives in simulated environments. The work bridges theory and practice to strengthen urban infrastructures against quantum threats. Future research can

address energy efficiency, sector interoperability, and federated learning for distributed detection. These advancements enhance the security and sustainability of next-generation urban systems [1].This paper presents lightweight Post-Quantum Cryptography (PQC), emphasizing its transition from traditional cryptographic schemes vulnerable to quantum threats to efficient PQC algorithms. Lattice-based cryptography, particularly CRYSTALS-Kyber and NTRU, is highlighted for IoT applications due to small key sizes , computational efficiency. However, integrating PQC into IoT faces challenges such as minimizing energy consumption, scalability, and hardware limitations. The review compares leading algorithms and explores optimization techniques to reduce resource overheads. Methods like algorithmic refinement, hardware acceleration, and hybrid cryptography are discussed to mitigate these challenges. The paper concludes that continued research is essential for the practical deployment of PQC in IoT systems, ensuring secure and scalable ecosystems in a post-quantum world [2]. multi-layered security framework to enhance Low Earth Orbit (LEO) communication systems, addressing current cybersecurity limitations. The framework combines quantum-resistant encryption, real-time anomaly detection using LSTM, and blockchain-based data logging to ensure confidentiality, integrity, and authenticity. It benchmarks quantum-enhanced AES against traditional encryption schemes, trains LSTM for anomaly detection, and assesses blockchain scalability. Results show significant improvements in anomaly detection performance but also highlight challenges like computational overhead and scalability. The framework offers potential for satellite communications and air traffic management, though further optimization and research are needed for better resource consumption and system resilience [3].

Web 3.0 aims to create decentralized ecosystems using blockchain technologies, driving digital transformation in commerce and governance. It enables secure and transparent services like digital identity, asset management, DAOs, and DeFi through consensus algorithms and smart contracts. As quantum devices evolve, Web 3.0 is existence developed alongside quantum cloud computing , quantum Internet. Quantum computing disrupts traditional cryptographic systems, reshaping modern cryptography with enhanced capabilities. This article explores quantum and postquantum advancements in blockchain, offering solutions like quantum-resistant signatures and quantum encryption algorithms to strengthen security. It also discusses the future potential of quantum blockchain in Web 3.0 , outlines key implementation strategies [4]. quantum computing threatens classical cryptographic systems relying on problems like integer factorization , discrete logarithm. This paper explores how quantum computers will impact cryptography, highlighting the need to upgrade cryptographic systems to defend against quantum attacks. It assesses the development of quantum-resilient algorithms, offering hope for securing data in the quantum era. Quantum algorithms challenge conventional cryptography, but post-quantum algorithms provide a potential solution [5].The Internet of Things has revolutionized device communication, with billions of interconnected devices becoming integral to everyday life. However, The IoT's rapid growth has heightened data security and privacy risks. Conventional lightweight cryptographic methods are vulnerable to quantum attacks, which can easily compromise classical encryption. Post-Quantum Cryptography presents a viable defense with quantum-resistant algorithms. This chapter explores the challenges of implementing PQC in resource-limited IoT devices, balancing computational efficiency with strong quantum threat resistance [6].

The convergence of blockchain and quantum computing creates both possibilities and risks for digital asset security. Blockchain's decentralized, tamper proof design is a core advantage, but its reliance on classical cryptography such as RSA , ECC makes it susceptible to quantum attacks. As quantum technology progresses, these threats grow more pressing, necessitating the adoption of post-quantum cryptographic solutions with protect blockchain integrity. Conversely, quantum computing could optimize blockchain performance by refining consensus protocols and boosting scalability. Ongoing research wrapped on developing quantum resistant cryptographic algorithms to safeguard blockchain networks against quantum attacks while simultaneously harnessing quantum computing capabilities to optimize performance. This dual approach aims to both mitigate security vulnerabilities posed by quantum technologies and exploit their potential to improve scalability and transaction processing speeds in blockchain infrastructures. This paper analyzes blockchain's quantum vulnerabilities, explores emerging defensive strategies, and assesses how quantum computing could strengthen blockchain infrastructure in a post-quantum era. [7].Quantum computing has sparked substantial research into quantum technologies, particularly in their applications within the financial sector. Quantum computing holds transformative potential for finance, enabling faster portfolio optimization, advanced fraud detection, and accelerated Monte Carlo simulations for pricing derivatives and assessing risk. The study also examines quantum computing's implications for blockchain and cryptocurrencies, analyzing how emerging quantum algorithms could reshape these technologies. By exploring these intersections, the research connects quantum advancements with practical financial applications, highlighting both opportunities and challenges for the industry. The research methodology involves analyzing quantum algorithms and their financial applications, based on a comprehensive review of academic sources. This paper highlights the latest findings and identifies open research questions for future development in the finance and quantum technology intersection [8].quantum resistant blockchain protocols leveraging post quantum cryptography, including lattice based, hash based, code based cryptographic solutions. We assess advanced consensus mechanisms such as Quantum-Secure Proof of Stake , Quantum-Protected Byzantine Fault Tolerance . Through simulation analysis, we demonstrate that these quantum safe blockchain architectures maintain robust security while ensuring efficient transaction throughput. Our research proposes a hybrid cryptographic framework blending classical and PQC components to achieve optimal security

performance balance for next generation blockchain systems [9].

Quantum computing threatens to disrupt traditional cryptography, rendering systems including RSA ,ECC vulnerable. Shor's algorithm, for instance, can solve integer factorization , discrete logarithms exponentially faster than classical methods, jeopardizing current security frameworks. It analyzes the mechanisms by which quantum systems undermine current encryption standards and explores emerging post quantum cryptographic strategies. The study also discusses the broader implications for data confidentiality, integrity, and trust across sectors like finance, healthcare, defense. Through literature synthesis and technical exploration, this paper emphasizes the need for transitioning to quantum-resilient cryptographic frameworks [10].The rapid advancement of artificial intelligence and quantum computing has created unprecedented cybersecurity challenges. AI is being weaponized to create convincing deepfakes, automate sophisticated malware, and enhance social engineering attacks, making cybercrime more accessible and dangerous. Simultaneously, quantum computing particularly through Shor's algorithm threatens to break widely-used encryption standards includes RSA , ECC, jeopardizing global data security. This report analyzes these converging threats and evaluates defensive strategies, including AI-powered detection systems and post quantum cryptographic solutions like lattice-based cryptography. As these technologies evolve, proactive adaptation of cybersecurity frameworks becomes critical to mitigate risks and protect digital infrastructure with ongoing efforts toward standardization and the need for global cooperation to secure the financial sector against future quantum and AI-driven threats [11].Quantum computing is poised to surpass classical computers, revolutionizing current processes. While it offers immense computing speed, it also presents risks, as malicious users could exploit this power to compromise systems. Quantum computing threatens RSA , ECC encryption, necessitating quantum-resistant algorithms still under development. While quantum key distribution (QKD) offers potential, it faces hardware and range limitations. This article examines these vulnerabilities and the ongoing efforts to address them through next generation cryptographic solutions.The cybersecurity community must collaborate to create effective post-quantum cryptography solutions [12].Cybersecurity has become crucial as cyberattacks grow more complex. This article explores how quantum computing, generative AI, and large language models (LLMs) intersect to transform cybersecurity. It examines how quantum-enhanced systems, AI-driven anomaly detection, and LLMs can improve cyber defense. The paper discusses their potential in protecting sensitive information and systems [13].

III. Quantum Algorithms and Their Impact on Cybersecurity

Quantum algorithms are revolutionizing field of cybersecurity by offering advanced methods for cryptanalysis, secure communication, and anomaly detection. Shor's algorithm threatens current encryption by factoring primes efficiently, while Grover's speeds up searches. Conversely, Quantum Key Distribution , BB84 leverage quantum physics for ultra-secure key exchange. These innovations present both risks and breakthroughs for cybersecurity. Moreover, quantum machine learning techniques are being explored for intrusion detection and anomaly recognition, while blockchain security is being strengthened with quantum approaches. This diverse application landscape highlights the critical role of quantum-resistant algorithms , secure multi-party computation in the future of cybersecurity.

A. Shor's Algorithm

Developed by Peter Shor in 1994, Shor's algorithm represents a fundamental breakthrough in quantum computing with profound implications for cybersecurity. This revolutionary algorithm efficiently solves two critical mathematical problems integer factorization and discrete logarithm computation that underpin modern public key cryptosystems including RSA, DSA, ECC. This capability threatens to undermine the security foundations of nearly all widely used public-key cryptography. The algorithm's theoretical potential has spurred urgent developments in post-quantum cryptography, as current encryption standards would become vulnerable with the advent of sufficiently powerful quantum computers. Moreover, researchers are actively developing quantum resistant cryptographic algorithms while security agencies worldwide are initiating transitions to these new standards. The cybersecurity implications extend across digital infrastructure, from secure communications to financial systems and blockchain technologies. As quantum computing technology advances, Shor's algorithm serves both as a landmark theoretical achievement and a practical warning, accelerating global efforts to develop and deploy quantum-resistant solutions. This technological paradigm shift constitutes perhaps the most critical challenge modern information security has faced, demanding a coordinated, global response from academia, industry, and government stakeholders to develop and deploy quantum-resistant safeguards for our digital infrastructure. [14].

B. Grover's algorithm

Grover's quantum search algorithm (1996) provides a quadratic speedup for unstructured search problems, reducing time complexity from classical $O(N)$ to quantum $O(\sqrt{N})$. While it does not fundamentally break symmetric cryptography, it effectively halves the security strength of algorithms like AES and SHA-3. For example, a 128-bit key becomes equivalent to 64-bit classical security, requiring the adoption of longer key lengths, such as AES-256, to maintain equivalent protection in the quantum era. For example, AES-128's security drops from 2^{128} to 2^{64} against quantum attacks. The algorithm achieves this through quantum parallelism, using amplitude amplification to boost the correct solution's probability. While less destructive than Shor's algorithm, Grover's speedup has prompted recommendations to double key sizes (e.g., adopting AES-256) for quantum resistance.

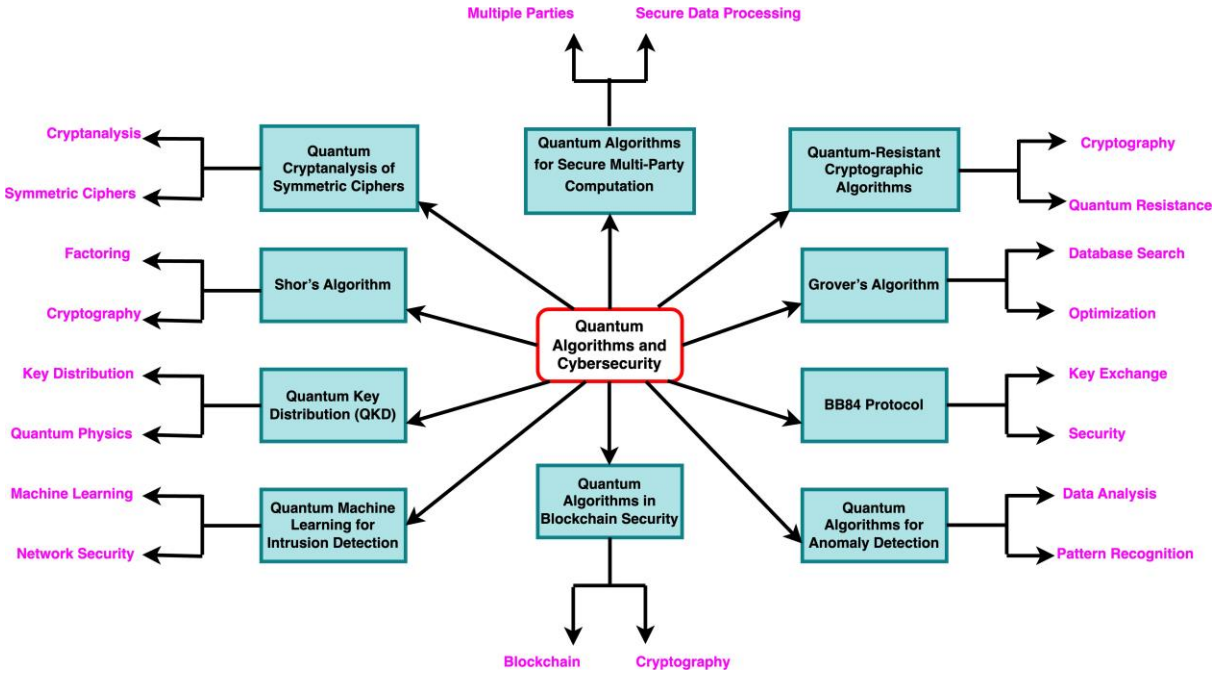

Fig. 1. Mapping Quantum Algorithms to Cybersecurity Challenges

This underscores the need to strengthen symmetric cryptography alongside developing post-quantum alternatives. still mandates proactive adaptations in symmetric and hash-based cryptography. As quantum computing matures, the relevance of Grover's algorithm continues to grow, emphasizing the need for quantum-resistant designs and security strategies in cryptographic applications to withstand both classical and quantum adversaries [15].

C. BB84 Protocol

The BB84 protocol, developed by Charles Bennett and Gilles Brassard in 1984, is a foundational quantum key distribution protocol. It allows two parties to establish a shared secret key by transmitting quantum states (typically photons) through a quantum channel, relying on superposition and the no-cloning theorem. Its security arises from quantum mechanical properties, which ensure that eavesdropping attempts introduce detectable disturbances, unlike traditional encryption methods relying on computational complexity assumptions. BB84 provides information-theoretic security rooted in physical laws rather than mathematical conjectures. This makes it inherently resistant to both classical and quantum computational attacks, including threats posed by Shor's algorithm against RSA encryption. The protocol operates by encoding bits in non-orthogonal quantum states, typically using photon polarization or phase encoding, with security verification performed through classical communication channels. As quantum computing advances threaten traditional cryptographic systems, BB84 has emerged as a critical component of quantum-resistant security infrastructures. While practical implementations face challenges such as distance limitations and detector vulnerabilities, ongoing advancements in quantum communication technologies continue to enhance its reliability and deployment feasibility. The protocol's theoretical robustness and growing technological maturity position it as a vital solution for securing communications in the post-quantum era, with current applications ranging from government and financial communications to the protection [16].

D. Quantum Key Distribution (QKD)

Quantum Key Distribution depicated a revolutionary advancement in cybersecurity, using quantum mechanical principles for theoretically unbreakable key exchange. By encoding information in quantum states (typically photon polarization), QKD ensures security by detecting eavesdropping, as any intrusion disturbs the system. BB84 protocol, developed by Bennett , Brassard in 1984, guarantees key confidentiality using photon superposition states and the no-cloning theorem. However, classical cryptography, which relies on computational complexity, QKD's security is based on quantum physics, making it resistant to both classical , quantum computing attacks. As quantum computers threaten to break traditional encryption methods like RSA, QKD emerges as a critical solution for protecting sensitive communications.

Current implementations demonstrate its viability for government, financial, and infrastructure security, though challenges remain in transmission distance and practical deployment. The protocol's information-theoretic security and ongoing technological improvements position QKD as an essential component of post-quantum cryptographic infrastructures, offering long-term protection against evolving Cybersecurity challenges in the quantum era. [17].

E. Quantum Machine Learning(QML) for Intrusion Detection

QML merges quantum computing with classical ML techniques, offering transformative potential for cybersecurity applications. By exploiting quantum superposition and entanglement, QML algorithms can process security-relevant datasets with unprecedented efficiency. In intrusion detection systems, quantum-enhanced approaches demonstrate three key advantages accelerated anomaly detection through parallel quantum processing, improved classification accuracy reducing false positives, and real time identification of sophisticated threats like zero-day exploits. Promising techniques include quantum support vector machines, quantum neural networks, quantum decision trees, which collectively enable faster pattern recognition in high-dimensional security data. While still in early development, QML represents a paradigm shift for defending against advanced persistent threats, potentially outperforming classical systems in both speed and detection capabilities as quantum hardware matures. This paper evaluates the impact of quantum algorithms on modern cybersecurity mechanisms, comparing their effectiveness with classical IDS techniques and exploring future directions for quantum-enhanced security systems [18].

F. Quantum Algorithms for Anomaly Detection

Quantum computing revolutionizes anomaly detection by overcoming classical ML limitations through quantum parallelism and entanglement. Quantum neural networks , support vector machines leverage superposition to simultaneously analyze multiple threat patterns, dramatically improving detection of APTs and zero-day exploits. These quantum-enhanced systems provide three key advantages: (1) higher precision in noisy environments, (2) reduced false positives via quantum-optimized classification, and (3) real-time processing of massive network traffic. Integration with existing IDS enhances cryptographic protocols and accelerates threat response. As quantum hardware advances, these techniques are becoming essential for post-quantum cybersecurity, offering exponential speedups in processing complex attack signatures. The maturation of quantum algorithms enables cybersecurity systems to preemptively address evolving threats, establishing a robust framework for future digital defense [19].

G. Quantum Cryptanalysis of Symmetric Ciphers

Quantum cryptanalysis exploits algorithms like Grover's to attack cryptographic systems, providing a quadratic speedup for symmetric-key attacks. While classical brute-force requires $O(2^n)$ operations for an n-bit key, Grover's algorithm reduces this to $O(2^{n/2})$, effectively halving the security margin of ciphers like AES. Although less dramatic than Shor's impact on asymmetric cryptography, this acceleration necessitates proactive defenses. The cryptographic community has responded with two key strategies doubling key lengths (e.g., AES-256) to restore $O(2^n)$ security against quantum brute-force, developing quantum-resistant symmetric primitives featuring enhanced nonlinear components, lattice-based structures, and quantum-secure pseudorandom functions. These solutions, now integrated into NIST's Post-Quantum Cryptography Standardization, balance backward compatibility with future-proof security. While current symmetric cryptography remains secure against classical attacks, these preparations ensure robust protection as fault-tolerant quantum computers emerge, maintaining both security and performance in the quantum era [20].

H. Quantum Resistant Cryptographic Algorithms

The rise of quantum computing critically endangers existing cryptographic protocols, with Shor's algorithm efficiently solving integer factorization discrete logarithm problems that underpin RSA , ECC encryption. This vulnerability necessitates urgent adoption of post quantum cryptography based on quantum resistant mathematical constructs, including lattice based , hash-based , code-based , multivariate polynomial systems. While these PQC solutions demonstrate theoretical security against quantum attacks, practical implementation faces challenges in performance optimization, standardization , and backward compatibility. Strategic migration requires systematic evaluation of these algorithms, development of hybrid transitional systems, and sustained research to address evolving threats while maintaining operational efficiency in cybersecurity infrastructure [21].

I. Quantum Algorithms in Blockchain Security

Blockchain systems face existential risks from quantum computing, as Shor's algorithm efficiently solves integer factorization , discrete alogarithms breaking RSA/ECC signatures in polynomial time, while Grover's algorithm quadratically expedite brute force attacks on symmetric cryptography. These capabilities directly threaten blockchain consensus mechanisms and transaction integrity. In response, three quantum resistant approaches are emerging lattice based cryptography such as CRYSTALS-Dilithium for digital signatures,hash based schemes like SPHINCS+ for tamper proof verification, code based alternatives such as BIKE for key encapsulation. Implementation challenges include maintaining blockchain's decentralized nature while accommodating larger key sizes and complex post-quantum operations. The blockchain community must prioritize hybrid cryptographic transitions combining classical and post quantum algorithms, quantum secure consensus protocol redesigns, proactive standardization through collaborations like NIST's PQC project. These measures are critical for preserving blockchain's immutability and trust model in the age of quantum computing. [22].

J. Quantum Algorithms for Secure Multi-Party Computation

Secure multi party computation empower multiple parties to collaboratively compute a function over their private inputs, ensuring that no party gains any information beyond their own input and the final output. Quantum algorithms present a promising avenue for enhancing SMPC protocols by leveraging quantum entanglement and superposition. Quantum techniques, such as quantum secret sharing , quantum homomorphic encryption, strive to enhance the efficiency and security of SMPC protocols.In classical SMPC, communication overhead and computational complexity can be significant, especially for large-scale systems. Quantum algorithms can potentially reduce these complexities by enabling faster computations and more secure protocols, even in the presence of malicious adversaries. Furthermore, quantum cryptographic primitives, like quantum key distribution, can strengthen the security guarantees of SMPC protocols. By integrating quantum algorithms into SMPC, cybersecurity systems can achieve robust, privacy-preserving computation that is resistant to both classical , quantum-based attacks [23].

IV. CONCLUSION

Quantum computing presents a paradigm shift for cybersecurity, simultaneously offering transformative potential and unprecedented threats. Our analysis reveals that quantum algorithms (Shor's , Grover's) fundamentally undermine classical cryptosystems breaking RSA/ECC via polynomial time factorization and reducing symmetric key security by half. This imminent vulnerability demands immediate transition to post quantum cryptography, including lattice based , hash based alternatives. We demonstrate that quantum key distribution, quantum enhanced security frameworks provide viable migration paths, though implementation challenges remain. Three critical action items emerge accelerated standardization of quantum-resistant algorithms, investment in hybrid cryptographic systems, development of quantum-secure protocols. These measures collectively address the urgent need to future proof digital infrastructure against quantum threats while harnessing quantum advantages. Our findings offer a strategic framework for safeguarding sensitive data in the post-quantum era.

REFERENCES

[1] Amna Khatoon and Rubina Riaz. Quantum computing impacts on smart city cybersecurity through resilient defense framework: Quantum computing impacts on resilient cybersecurity frameworks for smart cities. *Ubiquitous Technology Journal*, 1(1):23–31, 2025.

[2] Liyth H Mahdi and Alharith A Abdullah. Fortifying future iot security: A comprehensive review on lightweight post-quantum cryptography. *Engineering, Technology & Applied Science Research*, 15(2):21812–21821, 2025.

[3] Makhabbat Bakyt, Luigi La Spada, Nida Zeeshan, Khuralay Moldamurat, Sabyrzhan Atanov, Assem Konyrkhanova, Nikolay Yurkov, Absalyam Kuanysh, Yertis Marat, and Alzhan Tilenbayev. Advanced cybersecurity framework for leo aerospace: Integrating quantum cryptography, artificial intelligence anomaly detection, and blockchain technology. *Journal of Robotics and Control (JRC)*, 6(2):695–714, 2025.

[4] Xiaoxu Ren, Minrui Xu, Dusit Niyato, Jiawen Kang, Zehui Xiong, Chao Qiu, Haipeng Yao, and Xiaofei Wang. Building resilient web 3.0 infrastructure with quantum information technologies and blockchain: An ambilateral view. *Proceedings of the IEEE*, 2025.

[5] Tejinder Sharma, Rishab Sharma, et al. Post-quantum cryptography for navigating challenges and exploring opportunities. *International Journal of Research and Review in Applied Science, Humanities, and Technology*, pages 14–21, 2025.

[6] Kinjal Acharya, Shefali Gandhi, and Purvang Dalal. Cyber-security of iot in post-quantum world: Challenges, state of the art, and direction for future research. *Advancing Cyber Security Through Quantum Cryptography*, pages 363–396, 2025.

[7] Ruksana Saeed and Gabrielle Wallace. Blockchain and quantum computing: Securing digital assets in the age of advanced cyber threats. 2025.

[8] Abha Satyavan Naik, Esra Yeniaras, Gerhard Hellstern, Grishma Prasad, and Sanjay Kumar Lalta Prasad Vishwakarma. From portfolio optimization to quantum blockchain and security: A systematic review of quantum computing in finance. *Financial Innovation*, 11(1):1–67, 2025.

[9] Er Vikhyat Gupta and Er Akshit Kohli. Quantum-secure blockchain protocols: Enhancing privacy in post-quantum cryptography. *World Journal of Future Technologies in Computer Science and Engineering (WJFTCSE)*, 1(1):55–65, 2025.

[10] Babatunde Akande. The impact of quantum computing on encryption: How quantum computers can break current encryption methods, such as rsa and ecc, and what this means for data security. 2025.

[11] Ahmed M Elmisery, Mirela Sertovic, Andrew Zayin, and Paul Watson. Cyber threats in financial transactions–addressing the dual challenge of ai and quantum computing. *arXiv preprint arXiv:2503.15678*, 2025.

[12] Muhammad Sajid Iqbal, Ahthasham Sajid, and Rida Malik. Cyber security in the post quantum computer era: Threats and perspectives. In *Emerging Trends in Information System Security Using AI & Data Science for Next-Generation Cyber Analytics*, pages 15–29. Springer, 2025.

[13] P Alok. Enhancing cybersecurity through quantum computing and ai: A multi-disciplinary approach.

[14] Oded Regev. An efficient quantum factoring algorithm. *Journal of the ACM*, 72(1):1–13, 2025.

[15] Jed Brody and Grant-Christopher Worthington Sykes. Grover's search algorithm: An approachable application of quantum computing. *The Physics Teacher*, 63(1):23–25, 2025.

[16] Tat-Thang Nguyen, Thanh-Toan Dao, and Nhu-Quynh Luc. Develop a quantum key distribution application based on the bb84 protocol combined with a classical channel. *Bulletin of Electrical Engineering and Informatics*, 14(2):1381–1390, 2025.

[17] V´ıctor Zapatero, A´ lvaro Navarrete, and Marcos Curty. Implementation security in quantum key distribution. *Advanced Quantum Technologies*, 8(2):2300380, 2025.

[18] Adam Kadi, Aymene Selamnia, Zakaria Abou El Houda, Hajar Moudoud, Bouziane Brik, and Lyes Khoukhi. An in-depth comparative study of quantum-classical encoding methods for network intrusion detection. *IEEE Open Journal of the Communications Society*, 2025.

[19] A Hammad, Mihoko M Nojiri, and Masahito Yamazaki. Quantum similarity learning for anomaly detection. *Journal of High Energy Physics*, 2025(2):1–25, 2025.

[20] Randy Kuang. Quantum permutation pad for quantum secure symmetric and asymmetric cryptography. *Academia Quantum*, 2, 2025.

[21] Faguo Wu, Bo Zhou, Jiale Song, and Lijia Xie. Quantum-resistant blockchain and performance analysis. *The Journal of Supercomputing*, 81(3):498, 2025.

[22] Rasha Hani Salman and Hala Bahjat Abdul Wahab. Using lotka-volterra equations and lightweight post-quantum algorithm to develop lightweight blockchain security. *Fusion: Practice and Applications*, 19(1):128–143, 2025.

[23] Min Hou and Yue Wu. Multiparty quantum private comparison using rotation operations. *Axioms*, 14(4):274, 2025.