Volume 2 No 6, 2026
Journal of Global Research in Multidisciplinary Studies (JGRMS)
Review Paper
Available online at https://saanvipublications.com/journals/index.php/jgrms/index

Quantum Computing for cybersecurity and Intelligent Threat Detection: A Survey

Mr. Sachin Manekar
Assistant Professor,
Department of Computer Sciences and Applications
Mandsaur University, Mandsaur
Sachin.manekar@meu.edu.in

***Abstract*—Quantum Computing is the technology of the future that could revolutionize today's computing and security. Quantum computers able to run complex calculations faster than classical computers, thanks to the principles of quantum mechanics, such as superposition, entanglement and quantum parallelism. In this paper, authors give an extensive overview of quantum computing and its application in cybersecurity. It introduces basic concepts of quantum computing such as qubits, quantum gates, quantum circuits, and highlights of some of the important quantum algorithms like Shor's algorithm and Grover's algorithm. The research also covers the use of quantum computing in improving cybersecurity by leveraging post-quantum cryptography, quantum machine learning, network security, and quantum intrusion detection systems. Furthermore, the paper explores the key challenges and limitations of quantum technologies, such as scalability, fault tolerance, quantum noise, and security concerns. Additionally, a comprehensive literature survey of the latest developments and research works of quantum computing and quantum security are given. The results show the potential of quantum computing to enhance cyber security, but also highlight the challenges that will need to be addressed in the future, as quantum computers become increasingly common and powerful.**

***Keywords*—Qubits, Quantum Threat Detection, Cryptographic Security, Quantum-Enhanced Networks, Fault-Tolerant Computing, Intelligent Cyber Defense.**

I. INTRODUCTION

In the contemporary digital era, the security of information systems and sensitive data has become a critical concern due to the increasing sophistication of cyber threats. Consequently, advanced technologies are required to ensure robust and future-ready cybersecurity frameworks [1]. Quantum computing is a revolutionary computing paradigm using the principles of quantum mechanics, which is expected to overcome the limitations of classical computers in solving complex problems in a more efficient manner [2]. The strong computational power can revolutionize different sectors such as health care, finance, logistics, scientific research, etc. But the rapid development of quantum computing also presents new challenges for today's cybersecurity solutions, especially current cryptographic methods. Due to these factors, quantum cybersecurity has become an area of interest for researching secure and resilient systems that can be made future-proof against quantum threats [3][4].

The rapid growth of digital technologies and networked systems has led to an unprecedented increase in the volume, variety, and velocity of data exchanged across computer networks [5][6]. Intrusion detection systems (IDS) play a fundamental role in addressing these challenges by continuously monitoring network traffic and system activities to identify malicious behavior [7]. Security logs, intrusion alerts, and network traffic records are often stored in MySQL databases, enabling efficient data management, analysis, and support for intelligent threat detection and cybersecurity monitoring [8]. Quantum computing has emerged as a promising technology with the potential to address some limitations of classical computing [9].

Traditional machine learning models, such as support vector machine (SVM), K-nearest neighbor (KNN), naive Bayes, logistic regression (LR), decision trees, clustering, and combined and hybrid methods have been widely used in Network Intrusion Detection Systems (NIDS). However, machine learning (ML) models often rely on handcrafted features, requiring domain expertise and extensive preprocessing to ensure optimal performance [10]. Deep Learning (DL), on the other hand, has shown great accuracy in detecting sophisticated network attacks [11]. This paper surveys the role of quantum computing in cybersecurity and intelligent threat detection, covering fundamental quantum concepts, key algorithms, cryptographic implications, current challenges, and emerging research directions for developing secure, scalable, and quantum-resilient cybersecurity solutions.

A. *Structure of the paper*

The paper is organized as follows: Section II introduces the fundamentals of quantum computing, while Section III explores its applications in cybersecurity. Section IV discusses key challenges, limitations, and future scope. Section V presents a review of recent literature, and Section VI concludes the study with major findings and future research directions.

II. FUNDAMENTALS OF QUANTUM COMPUTING

Quantum Computing is an advanced quantum technology that is based on the use of qubits, superposition and entanglement to carry out computations that go beyond the capabilities of classical computers.

A. *Quantum Bits (Qubits)*

Quantum bits (qubits) are the building blocks of quantum computers, which are smaller than classical bits, but feature a capacity to occupy two or more states at once by means of superposition. Classical systems would only be able to represent the information as a 0 or a 1, while a qubit can be both simultaneously. Different physical implementations have

been suggested for the realization of qubits including superconducting circuits, trapped ions, photonic systems, neutral atoms, nitrogen-vacancy centers and semiconductor quantum dots. The state of a qubit is expressed as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, with the probability amplitude α and β being complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$.

B. Quantum Superposition and Entanglement:

Superposition and entanglement are fundamental principles of quantum computing that distinguish quantum systems from classical computing models. These properties enable quantum computers to process information in ways that are not possible with classical bits.

- **Superposition:** It allows qubits to exist in linear combinations of basis states until measurement collapses them. Unlike classical probability, superposition enables interference—constructive and destructive—allowing quantum algorithms to amplify correct results. For example, three qubits can simultaneously represent eight states that can be manipulated together by quantum operations. The geometry of superposition on the, where a qubit's state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is represented by polar and azimuthal angles θ and φ on the sphere's surface.
- **Entanglement :** A uniquely quantum phenomenon in which two or more qubits become correlated such that the state of one determines the state of the others, regardless of spatial separation. This property underpins many quantum algorithms and communication protocols [12]. A well-known example is the Bell state, $(|00\rangle + |11\rangle)/\sqrt{2}$ (QPMC). Without entanglement, many quantum algorithms would lose their exponential advantage.

C. Quantum Gates and Quantum Circuits:

Quantum gates are the basic building blocks of quantum circuits that operate on one or more qubits to manipulate quantum states and perform computations. Quantum gates are represented either as (i) unitary matrices or (ii) schematic diagrams.

- **Clifford + T Gate Set:** Quantum gates are represented either as (i) unitary matrices or (ii) schematic diagrams. shall focus on the Clifford+T gate set because it is (i) an approximately universal set and (ii) they can be made fault tolerant with existing quantum error correcting codes. Gates such as the Hadamard gate or T gate are examples of gates which produce a superposition state at the end of computation. Access to gates which produce superpositions enables the quantum circuit designer to execute a richer set of possible computations.
- **CNOT (Controlled Not) Gate:** Gates such as the Hadamard and T gate are called one qubit gates and the CNOT gate is an example of a two-qubit gate. The CNOT gate (or Controlled NOT gate) is a two-input operation where one input is referred to as the control qubit and the second input is the target qubit. When $|A\rangle = 1$, $|B\rangle$ shall have the value $1 \oplus B \equiv B$. When $|A\rangle = 0$, $|B\rangle$ shall be unchanged at the end of computation. The CNOT gate is an example of a controlled gate because the action of the gate (the NOT operation) is controlled by the value of qubit $|A\rangle$. The CNOT gate is also referred to as a Feynman gate in the literature.
- **Toffoli Gate:** The Toffoli gate takes 3 inputs A, B, C and returns 3 outputs A, B, $A \cdot B \oplus C$. The Toffoli gate is another example of a controlled gate. Unlike the CNOT gate, the Toffoli gate has two control qubits. The result of computation $A \cdot B \oplus C$ requires that two values simultaneously be 1 before C is complemented. Therefore, there are instances where the Toffoli gate is referred to in the literature as a doubly controlled CNOT gate or as a CCNOT gate.
- **Fredkin Gate:** The Fredkin gate takes 3 inputs A, B, C and returns 3 outputs A, $A \cdot B + A \cdot C$, $A \cdot B + A \cdot C$. When the control input A = 1, the values on inputs B and C are interchanged (or swapped) [13]. When A = 0, the values at inputs B and C are unchanged. As a result, the Fredkin gate is also referred to as a Controlled Swap gate or CSWAP gate.

D. Quantum Algorithms (Shor's and Grover's Algorithms):

Quantum algorithms utilize the principles of quantum mechanics to solve computational problems more efficiently than classical algorithms. Shor's and Grover's algorithms are among the most important quantum algorithms with applications in cryptography and search optimization.

- **Shor's Algorithms:** Shor's algorithm is used to factor large integers, a problem that cannot be solved efficiently by classical computers, which is why Shor's algorithm is used. It is polynomial time factorable, and has many applications in cryptography. The applications of quantum computing are not limited to the fields of information and communication technology, but quantum computers could also be used for cryptography, material science, chemistry, and artificial intelligence.
- **Grover's Algorithm:** In 1996, Lov Grover invented Grover's algorithm, which offers the best quadratic speedup improvement over classical algorithms for searching an unsorted database. Classical computing requires O(N) operations, whereas Grover's algorithm requires $O(\sqrt{N})$ operations [14]. It takes advantage of quantum amplitude amplification to boost the chances of obtaining the correct answer.

III. Application of Quantum Computing In Cybersecurity

Quantum computing is transforming cybersecurity by introducing new cryptographic challenges and enabling advanced techniques for threat detection, network security, and intelligent intrusion detection systems.

A. Post-Quantum Cryptography:

The three commonly used cryptographic systems in digital communication are RSA, Elliptic Curve Cryptography (ECC) and symmetric key algorithms. These algorithms are used to ensure the security of data transmission, which means that the information is transmitted in a way that prevents unauthorized access [15]. The development of quantum computers poses a threat to existing public-key cryptographic protocols, however, since quantum algorithms can efficiently break traditional encryption techniques [16].

B. Quantum Machine Learning for Threat Detection:

Today, Quantum Machine Learning has emerged as a promising approach that combines conventional machine

learning models with quantum computing, where computationally intensive tasks are executed on quantum devices to improve efficiency and performance.

- **Quantum Support Vector Machine:** One of the fundamental supervised ML methods designed to classify objects into two classes {-1, +1} is a support vector machine. Thus, theoretically, the training process of a binary classifier can be exponentially accelerated if the described classification algorithm is run on a quantum computer. This capability has motivated researchers to adapt SVM-based intrusion detection systems to quantum devices and evaluate their performance on large cybersecurity datasets. The implementation of the QSVM algorithm in IBM Circuit Composer is shown in Figure 1.

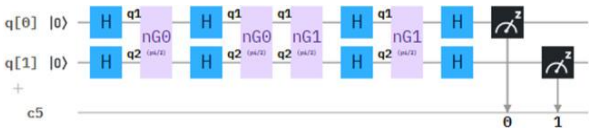

Fig. 1. QSVM circuit model

Figure 1 illustrates the QSVM implementation in IBM Circuit Composer, where quantum gates and qubits are used to process input data and perform classification tasks.

- **Quantum convolutional neural network:** A success case of quantum neural network that has demonstrated its quantum advantage in recognition of complex objects. When it comes to image processing, a CNN generally consists of a sequence of different (interleaved) layers of image processing; in each layer, an intermediate two-dimensional array of pixels, called a feature map is produced from the previous one. A CNN consists of different types of layers: convolutional layers, subsampling (or pooling) layers and layers of regular perceptron [17]. The first two layers (convolutional and subsampling) alternating with each other, form an input feature vector for a multilayered perceptron. The effectiveness of QCNN has encouraged researchers to develop QCNN-based intrusion detection systems and evaluate their performance on large datasets. Figure 2 presents a general QCNN's circuit model.

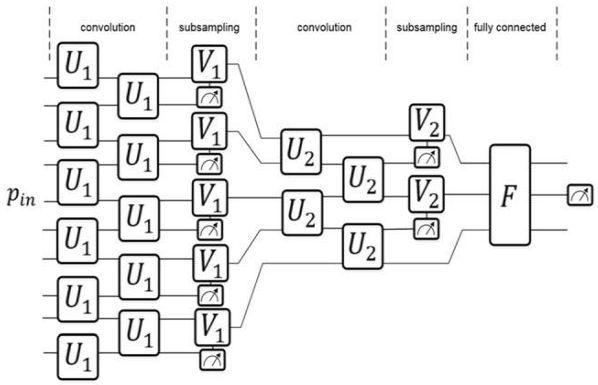

Fig. 2. QCNN circuit model

Figure 2 illustrates the general QCNN architecture consisting of convolution, subsampling, and a fully connected layers that process input quantum states and generate classification outputs.

C. Quantum Computing in Network Security:

It utilizes quantum principles such as superposition, entanglement, and quantum parallelism to address computational challenges in analyzing large-scale network data and detecting malicious activities. It supports quantum-enhanced algorithms for network anomaly detection, secure multiparty computation, and quantum-based cryptographic protocols to ensure data integrity and confidentiality. QML offers significant potential for improving network security by addressing complex and evolving cyber threats [18]. It can enhance threat intelligence through rapid analysis of network logs, threat feeds, and historical attack patterns [19]. Furthermore, QML contributes to the development of adaptive intrusion detection systems (IDS) capable of autonomously learning and responding to new and unknown threats in real-time.

D. Quantum-Enhanced Intrusion Detection Systems (IDS):

The growing adoption of Internet of Things (IoT) applications and remote access infrastructures has introduced several security vulnerabilities, increasing the need for advanced intrusion detection systems. Distributed Denial of Service (DDoS) attacks are among the major threats affecting networks by generating large volumes of unusual traffic that overwhelm hosts and consume system resources through malicious packets. As a result, legitimate users may gradually be denied access to network services. Various techniques have been developed to detect such anomalies. Since quantum systems possess high computational power, quantum intrusion detection systems can outperform traditional intrusion detection approaches [20]. Therefore, in real-time network applications, quantum intrusion detection systems are highly significant because they can detect anomalies quickly and help prevent major damage to network infrastructures.

IV. Challenges and Limitations

There are several challenges and limitations associated with the implementation of quantum computing in cybersecurity, as discussed below:

A. Hardware and Scalability in Quantum Computing:

Fault-tolerant quantum computing refers to the ability of a quantum computer to perform computations accurately despite errors caused by noise and imperfections in quantum hardware. As quantum computing continues to evolve, achieving fully fault-tolerant systems becomes increasingly important. Quantum systems face challenges due to noise, decoherence, and hardware-related errors, which can affect computational reliability. Overcoming these obstacles is essential for realizing the full potential of quantum computing. Scalability is another major challenge, as managing qubits, reducing noise, and maintaining coherence become more difficult as system size increases. Furthermore, quantum processors require ultra-low temperatures and become increasingly complex to manage as the number of qubits grows, making large-scale and reliable quantum computing a significant research challenge [21].

B. Operational Constraints of Current Quantum Systems:

Current quantum computing systems face several limitations, including correlated noise, qubit leakage, and crosstalk effects. These challenges affect fault tolerance,

system stability, and scalability, making reliable large-scale quantum computation difficult to achieve.

- **Correlated Noise and Fault Tolerance:** A central challenge is that QEC thresholds are not fixed values; they depend on the properties of the quantum error-correcting code and can undermine scalability even when average error rates appear low. Practical studies show that correlated structures must be explicitly modeled and ideally, exploited-either by adapting the decoder or by engineering the device so that correlations are suppressed or reshaped into less harmful forms. This suggests that fault tolerance is not only about reducing error magnitude but also about shaping error geometry relative to the code.
- **Leakage as a Scaling Controller**: Leakage is considered a major challenge because it behaves like an error mode that QEC is not naturally designed to correct. Leakage can corrupt multiple syndromes, propagate through gates, and persist. Overcoming leakage in QEC has therefore become a major line of research. In practical terms, this means that any platform with significant leakage must include fast and reliable leakage detection, active reset, and decoding that accounts for leakage-induced syndrome anomalies.
- **Crosstalk and Calibration Limitations:** As devices scale, crosstalk can introduce conditional errors and create spatially extended error patterns. In addition, frequent recalibration interrupts computation, while insufficient recalibration allows drift to increase error rates during long QEC runs [22]. Thus, scalability requires not only good qubits, but also a stable and automatable control stack.

C. Cybersecurity Risks in the Quantum Era:

The advent of quantum computing presents significant security challenges to traditional cryptographic systems. Many existing cryptographic algorithms used to protect critical infrastructure and confidential data may become ineffective against quantum computer attacks. Organizations that delay the adoption of quantum-resistant cryptographic methods remain vulnerable to threats such as cryptographic breaches, identity theft, financial fraud, and cyber espionage. Classical security systems are particularly at risk because quantum computing can solve certain mathematical problems that form the foundation of modern cryptography [23]. Consequently, future quantum attackers may be able to break widely used encryption algorithms. Quantum algorithms such as Shor's and Grover's algorithms have the potential to compromise cryptographic security by recovering private keys, decrypting sensitive information, and gaining unauthorized access to confidential data, emphasizing the need to reassess existing security frameworks in preparation for the quantum era.

V. LITERATURE REVIEW

The literature review examines recent advancements in quantum computing and cybersecurity, focusing on quantum machine learning, intrusion detection, quantum communication, cybersecurity frameworks, implementation challenges, and future research opportunities.

P. Kamble et al. (2026) proposed a Hybrid Deep Learning–Decision Tree (DL-DT) model that improved cyber-attack detection accuracy, efficiency, and latency by integrating rule-based frequency filtering. However, the framework was validated on a single dataset, limiting its generalizability. Future studies should evaluate its performance across diverse, real-time cybersecurity environments [24].

Y. Zhu et al. (2026) proposed single-qubit quantum graph neural networks (sQGNNs) to enhance graph learning performance and computational efficiency. However, their evaluation was limited to benchmark datasets. Future studies should focus on large-scale deployment and validation on practical quantum computing platforms [25].

G. J. Skulmoski and A. Memari (2025) presented quantum cybersecurity program management strategies to improve organizational readiness. However, the work primarily emphasizes planning and governance rather than implementation. Future studies should investigate practical deployment, effectiveness, and scalability of quantum-safe cybersecurity frameworks in diverse environments [26].

I. Mahmud and A. Abdelhadi (2025) reviewed the integration of Artificial Intelligence in Quantum Communication to improve security, transmission reliability, and network scalability. The study analyzed machine learning techniques, including neural networks and reinforcement learning, and highlighted the need for unified, cost-effective, and scalable AI-driven quantum communication frameworks [27].

S. Sankar, R. Dutta, and S. Karmakar (2024) examined different machine learning methodologies for predictive analysis and cyber threat assessment, leveraging data-driven methodologies to bolster early detection and automatic responses to evolving network attacks. Furthermore, the work points out various key challenges in implementation, including data privacy, explain ability of models, and protection against adversarial attacks [28].

D. Abreu, C. E. Rothenberg, and A. Abelém (2024) proposed QML-IDS for enhanced attack detection and classification performance. However, its practical applicability remains uncertain due to limited real-world validation. Future studies should investigate scalability, computational requirements, and deployment in dynamic cybersecurity infrastructures [29].

The Table I summarizes the major studies related to quantum computing in cybersecurity, presenting their key contributions, techniques, advantages, limitations, and recommendations for future research.

TABLE I. SUMMARY OF LITERATURE REVIEW ON QUANTUM COMPUTING AND CYBERSECURITY APPLICATIONS

Authors	Study on	Contributions	Advantages	Limitations	Recommendations
Y. Zhu et al., (2026)	Single-Qubit Quantum Graph Neural Networks (sQGNNs)	Proposed efficient graph-learning architecture for NISQ-era quantum systems	Improved scalability, efficiency, and generalization capability	Requires further validation on larger quantum hardware	Explore large-scale deployment and advanced quantum architectures

G. J. Skulmoski and A. Memari (2025)	Quantum Cybersecurity Program Management	Presented risk-based frameworks for quantum-safe cybersecurity adoption	Supports organizational preparedness for quantum threats	Focused mainly on governance and implementation strategies	Accelerate practical deployment of quantum-safe security frameworks
I. Mahmud and A. Abdelhadi (2025)	Artificial Intelligence in Quantum Communication	Reviewed the integration of AI techniques in quantum communication systems	Improved security, transmission reliability, and network scalability	Lack of unified, cost-effective, and scalable implementation frameworks	Develop standardized, cost-effective, and scalable AI-driven quantum communication frameworks
S. Sankar, R. Dutta, and S. Karmakar (2024)	Machine Learning for Cyber Threat Asent	Reviewed predictive analytics and automated threat detection techniques	Supports early threat detection and response automation	Privacy, explainability, and adversarial attack concerns remain	Develop more secure and explainable ML-based security models
D. Abreu, C. E. Rothenberg, and A. Abelém (2024)	Quantum Machine Learning Intrusion Detection System (QML-IDS)	Proposed a hybrid quantum-classical intrusion detection framework for network security	Improved attack detection in binary and multiclass scenarios	Requires validation in real-world large-scale environments	Evaluate framework on diverse and real-time network datasets

VI. Conclusion and Future Work

As one of the most promising technologies to transform the cybersecurity landscape in the years to come, quantum computing is rapidly gaining traction. Quantum computer technology can be used to create new secure communication systems, smarter threat detection systems, and more sophisticated security systems by leveraging the principles of quantum mechanics, including superposition and entanglement. This review emphasized the key principles of quantum computing, its potential applications in cybersecurity, and the emerging field of quantum machine learning for tackling complex security problems. In addition, the study revealed challenges that currently prevent the widespread adoption of large-scale implementations, such as hardware limitations, quantum noise, scalability, operational complexity and high implementation costs. Despite these difficulties, ongoing developments in quantum technology suggest great promise for quantum-enhanced cybersecurity systems. Future research should focus on quantum-safe cryptography, fault-tolerant quantum systems, AI-driven threat detection, and secure blockchain integration. Collaborative efforts among researchers, industry, and policymakers will be essential to developing scalable, resilient, and practical quantum-enabled cybersecurity infrastructure to address emerging cyber threats.

References

[1] H. P. C. Shiva Kumara, "Deep Learning-Based Intrusion Detection and Cybersecurity Framework for Connected Vehicle CAN Bus Communication Networks," in *2026 14th International Symposium on Digital Forensics and Security (ISDFS)*, Boston, MA, USA: IEEE, 2026, pp. 1–6, March. doi: 10.1109/ISDFS69419.2026.11459074.

[2] H. E. Kodagoda, "FUNDAMENTALS OF QUANTUM COMPUTING IN CYBERSECURITY," 2026, *ResearchGate (Preprint)*. doi: 10.13140/RG.2.2.28364.68487.

[3] V. K. Bollu, "Threat Landscape in Artificial Intelligence Systems: Taxonomy, Attack Vectors and Security Implications," *World J. Adv. Res. Rev.*, vol. 29, no. 1, pp. 285–294, 2026, doi: 10.30574/wjarr.2026.29.1.0007.

[4] R. V. S. S. B. R, R. R. Al-Fatlawy, S. M. Sundaram, E. A. Rathnakumari, and M. Sudha, "Quantum variational based support vector machine for early detection of sepsis," in *2024 4th International Conference on Mobile Networks and Wireless Communications (ICMNWC)*, Tumkuru, India: IEEE, 2024, pp. 1–5, December. doi: 10.1109/ICMNWC63764.2024.10872228.

[5] A. Kaissar and A. B. Nassif, "Enhancing Network Intrusion Detection with Quantum Machine Learning: A Comprehensive Survey of Methods, Metrics, and Applications," *Futur. Internet*, vol. 18, pp. 1–27, 2026, doi: 10.3390/fi18050234.

[6] S. Sen, "Data Stewardship: How AI Agents Form the Pillars for Effective Data and AI Governance," *Int. J. Emerg. Trends Comput. Sci. Inf. Technol.*, vol. 5, pp. 151–155, 2024, doi: 10.63282/3050-9246.IJETCSIT-V5I4P117.

[7] S. Singh, "Advancing Network Security in 5G: Leveraging the 5G-NIDD Dataset for Intrusion Detection and Mitigation," in *2025 IEEE 12th International Conference on Cyber Security and Cloud Computing (CSCloud)*, IEEE, Nov. 2025, pp. 1–6. doi: 10.1109/CSCloud66326.2025.00055.

[8] H. B. Dama, "A Survey of MySQL Database Administration Techniques and Best Practices," *ESP J. Eng. Technol. Adv.*, vol. 6, no. 1, pp. 89–98, February, 2026.

[9] A. Gupta, "What Is The Right Security Posture? A Perspective on Cloud Computing Security Threats and Risk Assessment," *Int. J. Emerg. Res. Eng. Technol.*, vol. 4, no. 4, pp. 120–127, December, 2023, doi: 10.63282/3050-922X.IJERET-V4I4P112.

[10] D. Chaudhary, S. Rajasegarar, and S. R. Pokhrel, "Towards Adapting Federated & Quantum Machine Learning for Network Intrusion Detection: A Survey," *arXiv Prepr.*, pp. 1–34, 2025, doi: 10.48550/arXiv.2509.21389.

[11] S. Kundu, T. Gupta, A. Sardar, A. Bandyopadhyay, and S. Swain, "A survey on quantum computing: Transforming cryptography, AI/ML, blockchain, and network communication," *Franklin Open*, vol. 12, no. April, p. 100371, 2025, doi: 10.1016/j.fraope.2025.100371.

[12] V. Raseena, "Quantum computing: foundations, algorithms, and emerging applications," *Front. Quantum Sci. Technol.*, vol. 4, no. December, pp. 1–15, 2025, doi: 10.3389/frqst.2025.1723319.

[13] Y. Guo, "Efficient quantum circuit compilation for near-term quantum advantage," *EPJ Quantum Technol.*, vol. 12, p. 69, 2025, doi: 10.1140/epjqt/s40507-025-00368-9.

[14] D. Krizhanovskyi, "An Overview of Quantum Algorithms: Detailed Analysis of the Deutsch-Jozsa and Grover's Algorithms," *SSRN Electron. J.*, no. August, 2024, doi: 10.2139/ssrn.4930685.

[15] M. H. Jebur and S. M. Khaleel, "Quantum Cryptanalysis: Evaluating the Impact of Shor's and Grover's Algorithms on Modern Encryption Standards," *CyberSystem J.*, vol. 2, no. 2, pp. 41–55, 2025, doi: 10.57238/csj.2025.1012.

[16] S. Kumara, "A Lightweight Deep Learning Based Classification Models for Non-Human Identity Threat Detection," in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, IEEE, Feb. 2026, pp. 1–6. doi: 10.1109/ICAIC67076.2026.11395886.

[17] M. Kalinin and V. Krundyshev, "Security intrusion detection using quantum machine learning techniques," *J. Comput. Virol. Hacking Tech.*, vol. 19, no. 1, pp. 125–136, 2023, doi: 10.1007/s11416-022-00435-0.

[18] D. Bhattacharjee, "Design and Evaluation of Deep Generative AI Model for Intrusion Detection in Cyber Threat Monitoring," in *2025 7th International Symposium on Advanced Electrical and Communication Technologies (ISAECT)*, 2025, pp. 1–6. doi: 10.1109/ISAECT68904.2025.11318752.

[19] R. Alluhaibi, "Quantum Machine Learning for Advanced Threat Detection in Cybersecurity," *Int. J. Saf. Secur. Eng.*, vol. 14, no. 3, pp. 875–883, 2024, doi: 10.18280/ijsse.140319.

[20] T. H. Kim and S. Madhavi, "Quantum intrusion detection system using outlier analysis," *Sci. Rep.*, pp. 1–13, 2024, doi: 10.1038/s41598-024-78389-0.

[21] M. Abughanem, "IBM quantum computers: evolution, performance, and future directions," *J. Supercomput.*, vol. 81, 2025, doi: 10.1007/s11227-025-07047-7.

[22] S. Ahmed, A. Ahad, and S. Subhan, "Decoherence Impediments in Quantum Computing and Fundamental Challenges of Quantum Error Correction," *Asian J. Res. Comput. Sci.*, vol. 18, no. 12, pp. 228–239, 2025, doi: 10.9734/ajrcos/2025/v18i12800.

[23] Y. Baseri, V. Chouhan, and A. Ghorbani, "Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure," *Comput. Secur.*, vol. 167, p. 104917, 2026, doi: 10.1016/j.cose.2026.104917.

[24] P. Kamble, M. Patane, A. Chandole, S. Dandge, and P. Lahande, "A Deep Learning Based Evolution of Decision Trees for Cyber Attack Detection," in *2026 13th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2026, pp. 1–6. doi: 10.23919/INDIACom70271.2026.11526518.

[25] Y. Zhu, R. Jiang, Q. Ni, and A. Bouridane, "Enable Quantum Graph Neural Networks on a Single Qubit With Quantum Walk," *IEEE Trans. Artif. Intell.*, vol. 7, no. 5, pp. 2496–2505, 2026, doi: 10.1109/TAI.2025.3592896.

[26] G. J. Skulmoski and A. Memari, *Quantum Cybersecurity Program Management*. Business Expert Press., 2025. doi: 10.1109/9781637427217.

[27] I. Mahmud and A. Abdelhadi, "Artificial Intelligence in Quantum Communications: A Comprehensive Survey," *IEEE Access*, vol. 13, pp. 121174–121205, 2025, doi: 10.1109/ACCESS.2025.3585799.

[28] S. Sankar, R. Dutta, and S. Karmakar, "Quantum Machine Learning: Recent Advances, Challenges, and Perspectives," in *2024 IEEE 21st India Council International Conference (INDICON)*, 2024, pp. 1–6. doi: 10.1109/INDICON63790.2024.10958346.

[29] D. Abreu, C. E. Rothenberg, and A. Abelém, "QML-IDS: Quantum Machine Learning Intrusion Detection System," in *2024 IEEE Symposium on Computers and Communications (ISCC)*, 2024, pp. 1–6. doi: 10.1109/ISCC61673.2024.10733655.

