Journal of Global Research in Electronics and Communication
Volume 1, No. 9, September 2025
Available Online at: www.jgrec.info
RESEARCH PAPER

Next-Generation Cybersecurity: The Role of AI and Quantum Computing in Threat Detection

Dr. Nilesh Jain
Associate Professor
Department of Computer Science and Applications
Mandsaur University
Mandsaur, India
nileshjainmca@gmail.com

***Abstract*—The high rate at which cyber threats are increasing requires the adoption of new security systems using new technologies. This research work focuses on the disruptive contributions of Artificial Intelligence (AI) and Quantum Computing to modern cybersecurity. Artificial intelligence-based security solutions are better at identifying threats, automating response and making them more resistant to advanced attacks, such as advanced persistent threats (APTs) and zero-day vulnerabilities. Until then, Quantum Computing is both a curse and a blessing; an opportunity to implement radical cryptographic protocols and secure communication, but a threat to traditional cryptography. Quantum Machine Learning (QML) is an AI and quantum algorithm that improves intrusion prevention and anomaly detection. There is much to do, including exploring the capabilities of quantum hardware, addressing the challenges of applying quantum security to existing infrastructures, and navigating the ethical issues of AI-based cybersecurity, despite these changes being underway. The answers to these issues lie in the holistic approach (technology, policy and education). In this paper, I provide an overview of current developments, solutions, and future studies in AI and quantum-enhanced cybersecurity and how they can revolutionize threat detection and defense systems in the digital age.**

Keywords*—*Cybersecurity, Quantum Computing, Encryption, Quantum Machine Learning, Threat Detection, Machine Learning.

I. INTRODUCTION

Cybersecurity has become essential to technological advancement in today's dynamic digital world. vulnerability to cyber-attacks escalates with the proliferation of networked technologies. Cybersecurity initiatives focus on data, infrastructure, and systems that are particularly vulnerable to cyberattacks, which can disrupt entire economies and communities. The growing frequency and complexity of these events necessitate a prompt reaction, especially in vital industries like healthcare, national security, and the financial industry [1]. There was a significant increase in associated expenditures by 2020, largely due to the substantial economic, operational, and reputational harm caused by cybercrime. Even while they are crucial, cyber defences like firewalls, anti-malware programs, and static encryption fall far short. Insider threats, human mistakes, and the massive amounts of data produced daily further complicate cybersecurity solutions. This highlights the necessity for innovation, flexibility, and proactive cybersecurity measures. Cyberattacks are becoming more complex; thus, they must reevaluate their defences. Emerging technologies like blockchain and AI have been developed to address the drawbacks of previous cybersecurity methods [2]. These technologies have the potential to bring forth more rapid, intelligent, and secure capabilities, which could completely alter the methods used to identify, prevent, and mitigate cyber threats. Automatic threat identification and incident response can only be achieved with the help of AI.

Quantum machine learning (QML) methods, including quantum support vector machines (SVMs) and variational quantum circuits, enhance threat detection by processing massive datasets more efficiently than traditional techniques. The emergence of artificial intelligence (AI) and quantum computing has changed the concept of cybersecurity [3] in a significant manner. Queen computing, combined with adaptive intelligence of AI, potentially allow these technologies to address cybersecurity issues that have thus far remained unsolvable with the introduction of quantum computing, AI models have become able to process data at the speed of light, responding quickly to threats.

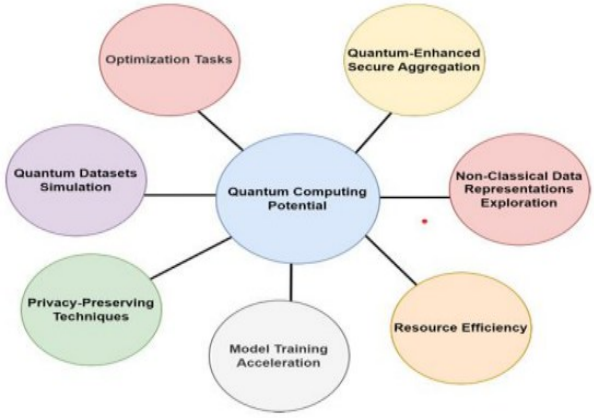

Fig. 1. Quantum Computing &AI Use in Cyber Security

The emergence of quantum computing, as shown in Figure 1, has significant implications for cybersecurity, particularly in encryption. The secure cryptography techniques RSA and ECC are predicated on how difficult it is to factor large numbers. Quantum computing can not only impact encryption but also improve threat design and mitigation in cybersecurity. Quantum computers make it possible to investigate large volumes of data, as well as nearly instantaneously identify patterns that point to cyber threats, through their unprecedented processing power [4]. In terms of security, AI can automate it with the assistance of quantum computing, which would be difficult to do with classical computing [5].

This approach involves constantly improving encryption algorithms based on threat level assessments in order to make cyber defence stronger [6]. Cyberattacks are always changing, so it's important to be able to quickly find and respond to them to limit the damage caused by security breaches. This is possible because data processing and pattern recognition are getting quicker.

A. *Structure of the Paper*

This paper is organized as follows: The use of AI in cyber defence is reviewed in Section II. Cybersecurity and Quantum Computing, Section III. Cyber Defence with AI and Quantum Computing, Section IV. Literature and case studies are reviewed in Section V, and future directions are discussed in Section VI.

II. Artificial Intelligence in Cybersecurity

The development of AI-based cybersecurity systems has transformed the approach of security professionals in safeguarding digital resources and combating cyberattacks. AI has progressed from its humble beginnings as a task Automator to a powerful tool for complex tasks, such as anomaly detection, pattern recognition, and predictive analysis, due to the effectiveness of ML. AI was first incorporated into cybersecurity models with the intention of automating mundane tasks to boost productivity and reduce human errors. The use of AI computers to identify network intrusions, malware, secure communications, phishing attempts, and security holes is illustrated in Figure 2. Nevertheless, sophisticated AI methods were required because rule-based algorithms failed to adequately react to complicated threats [7]. ML techniques, which enable AI systems to acquire new skills by analyzing existing data, are widely used as a result.

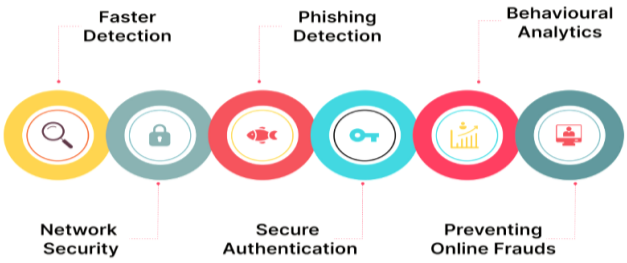

Fig. 2. AI in cybersecurity

By utilizing ML techniques, AI systems are able to sift through mountains of data in search of security concerns, giving those in charge of risk mitigation a leg up. In addition to performing predictive analysis, these algorithms help security professionals prevent security breaches by predicting when they might happen. The rise in popularity of natural language processing and similar AI technologies is a direct result of this shift in AI activities [8].

A. *AI-Driven Intrusion Detection Systems (IDS)*

The theoretical framework for AI-driven IDS is grounded in principles from both ML and cybersecurity domains. Fundamentally, the framework is founded on the following important components:

1) *Machine Learning Algorithms*

AI-powered IDs employ a variety of ML algorithms, such as neural networks, support vector machines, decision trees, and clustering, among others. Labelled datasets are used to train these algorithms to differentiate between benign and detrimental behaviours. These datasets contain both typical and unusual patterns of network traffic.

2) *Feature Extraction and Selection*

In order to get insight into the network's behaviour, feature extraction algorithms transform the raw network data into usable representations. To overcome the challenges of dimensionality and computing complexity, feature selection approaches make it easy to determine which features are most discriminative in identifying intrusions.

3) *Cyber Threat Intelligence Integration*

Cyber threat intelligence feed integration gives AI-driven intrusion detection systems context about known threats, malware signatures, and compromise indicators [9]. A higher detection rate and the ability to priorities security alerts based on threat severity can be achieved by integrating these systems with external sources of threat intelligence.

4) *Model Interpretability and Explainability*

The trust and awareness that security professionals gain from AI-driven intrusion detection system models depend on their interpretability and explainability. For stakeholders to grasp the model's predictions and assess the reliability of the intrusion detection results, tools like decision trees and model-agnostic interpretability methodologies are utilized.

5) *Supervised ML for Intrusion Detection*

Data output from an ML task is translated using input-output pair relationships. In this empirical study have taken into account popular machine methods for intrusion detection [10]. Using the training data, the primary goal of supervised learning is to achieve a specific objective. Typical tasks with this learning style include regression and classification processes.

B. *Applications of AI in Cyber Security*

Applications of AI provide substantial benefits for the creation and management of secure networking and system monitoring; yet, as interest in AI grows, the inherent risks and weaknesses damage the technology's reputation.

1) *Threats Detection and Prevention*

Cybersecurity relies on the identification and prevention of threats, and AI is utilized to enhance these capabilities. For the purpose of detecting malware, phishing, or insider risks, such systems are able to efficiently analyze massive amounts of data [11]. AI is a powerful tool in the battle against threats because of its ability to sort through data in real-time. Conventional approaches, which depend on already established regulations, are laborious and wasteful. By constantly learning from new data and identifying trends and patterns that humans might miss, AI is able to swiftly adapt to emerging threats.

2) *Anomaly Detection*

Critical to cyber defence is anomaly detection, which seeks dangers that do not fit the pattern of typical systems or networks. AI advancements are opening the door to improved threat identification and response in this field. Information from various sources, such as network traffic, user behaviour, and system logs, can be processed by AI-driven systems. Unlike the human mind, they can detect subtle irregularities. Anomalies like these teach AI to learn and grow, which gives it a leg up when faced with new and more hazardous dangers [12]. Algorithms powered by AI are faster than static rule-

based systems in learning from mistakes and adjusting to evolving risks. Anomaly detection might benefit from AI's ability to reduce false positives while also identifying genuine outliers. It can gather data from several sources, which helps pinpoint dangers with an adequate degree of detail while minimizing the impact of false warnings. Additionally, AI aids in the detection of rapidity and precision by analyzing data as events occur, allowing the company to respond swiftly to early-stage danger identification.

3) Vulnerability Management

The cyber security system also includes vulnerability management, which is responsible for finding, analyzing, and reducing vulnerabilities. A vulnerability is any hole, imperfection, or weakness in the system or application. Also, AI has automated a lot of vulnerability detection approaches, which helps businesses find and fix security holes according to importance [13]. AI is also useful for vulnerability control, as it ranks threats based on their level of safety or risk. Algorithms powered by AI can sort vulnerabilities according to their risk score and potential for compromise. The vulnerability scanning and protection procedure can be automated using this technology, reducing the need for human intervention.

4) User Authentication

Access control is one of the most crucial components of cybersecurity, as it ensures that only authorized individuals can access systems and data. Additionally, AI has enhanced user authentication technology, facilitating the adoption of safe and efficient practices by organizations. AI is widely used in biometric authentication as weight sensors can analyze client biometric data (such as speech recognition, fingerprints, and facial scans) in place of physical contact. Since biometric information is unique and difficult to counterfeit, these systems offer security characteristics that surpass those of password-based techniques.

5) Threat Intelligence

The procedures that entail obtaining, evaluating, and comprehending data on current or potential cyberthreats are referred to as cyber threat intelligence [14]. It helps organizations' triage processes discover the actors' tactics, methods, and plans (TTPs) in order to find the best solutions for more secure systems and data. Figure 3 shows how AI has automated data flow across several organizations from hazard detection to counter threat, thus revolutionizing risk intelligence.

Fig. 3. Cyber Security in different organization.

III. Quantum Computing and Cyber Security

A revolutionary quantum computing, a shift in computational theory, employs ideas from quantum mechanics to complete activities that conventional computers were previously unable to perform. Quantum computers apply the laws of quantum physics to perform a complex computation at unprecedented speed [15]. In the field of cybersecurity, technology and quantum computing provide both opportunities and hazards. On the one hand, quantum technologies can be employed to secure the encryption schemes, however, on the other, they can be employed to undermine them too [16]. This duality highlights the importance of detailing and analyzing the possible advantages, disadvantages, implications, and risks of quantum computing integration in cybersecurity procedures.

A. Advancements in Quantum Computing and Its Impact on Cybersecurity

The rapidly developing technology of quantum computing has the potential to revolutionize a number of industries, including cybersecurity. The quantum computers have an un-matched processing power that can perhaps reduce the current encrypting systems compared to the classic computers, which are incapable to handle higher end encryption programs.

One of the most remarkable features of quantum computing, one should single out the fact that quantum computing utilizes the entanglement and superposition properties of quantum physics. These properties enable processing a vast number of states at a high level of capability [17]. In this way, the completion of a task might take centuries with classical computers and only seconds or minutes with quantum machines.

These advances have radical consequences on cybersecurity. The majority of the currently used encryption algorithms are based on the complexity of large prime number factors. However, with sufficient computational power, these algorithms can be compromised, and quantum computers are available. RSA and ECC are public-key cryptography protocols frequently used in online transactions and communications that are considered to be safe [18][19]. The impact of this weakness can be enormous. Confidential information in all sectors, including financial institutions that store client data and government organizations responsible for protecting secrets, may be at risk if thieves attempt to use quantum computing to decrypt encrypted data.

B. Quantum Computing in Anomaly Detection and Pattern Recognition

The ability of Quantum computing has been noted by its capacity to detect anomalies in large volumes of data. Abnormalities of various types can be easily detected by quantum parallelism when multiple instances are tested simultaneously. This enables unusual events and trends to be spotted faster with these so-called quantum-enhanced anomaly detectors [20]. To illustrate, quantum principal components analysis (QPCA) tools developed to work with quantum data sets could be clustered and their dimensionality reduced through ML. This type of analysis also gives a clue as to what would be considered an anomaly. Moreover, quantum computers are also useful in overcoming the problems of complexity and high-dimensional space when performing pattern recognition.

Classical pattern recognition methods often struggle to create feature structures in high-dimensional spaces due to the curse of dimensionality. To overcome the issue, however, quantum computing may encode data as quantum states, and pattern recognition algorithms such as QNN can be applied more cost-effectively. Moreover, these advanced methods have significantly improved the speed and accuracy of pattern recognition tasks. They are becoming increasingly important to renowned authorities in fields such as signal analysis, image recognition, and NLP.

C. *Real-World Applications of Quantum Computing*

These applications highlight the disruptive potential of quantum computing across various sectors. As technology matures, its integration with AI and deep analytics continues to enhance efficiency, security, and decision-making capabilities even further, as illustrated in Figure 4.

Fig. 4. Real-World Applications of Quantum Computing

- **Cyber security & Cryptography**: The growing number of cyberattacks happening every day throughout the world has left the online security sector extremely exposed. Establishing a security framework in an organization is essential, but it can be a demanding and impractical task for traditional digital systems [21]. Therefore, cybersecurity remains a critical issue globally. In addition to becoming more susceptible to these dangers, reliance on digital technologies is growing. Combining ML with quantum computing can help create a variety of countermeasures for various cybersecurity threats. The creation of quantum cryptography, a technique for encryption, is another use of quantum computing.
- **Financial Modelling:** In order to stay afloat, the financial sector must choose the optimal combination of investment opportunities, taking into account anticipated returns, risk, and other criteria. To achieve this, traditional computers are constantly running "Monte Carlo" simulations, which take up a lot of computing resources. Companies can use quantum technology to do these huge and complicated calculations, thereby improving solution quality and reducing development time. Even a slight increase in projected return can have a significant impact on financial executives when they are managing billions of dollars.
- **Logistics Optimization:** Improved data analysis and rigorous modelling may help many different sectors enhance supply-chain management logistics and scheduling procedures. Applications can be significantly impacted by the necessity to always find and reevaluate transportation management within operational models, the optimal routes for freight, distribution, air traffic control, and fleet operations. A conventional computer is typically employed to do these jobs. However, a quantum technique could potentially tackle some of the more challenging ones.
- **Drug Design & Development**: A drug's design and development present one of quantum computing's most formidable challenges. The conventional approach to drug development involves a lot of trial and error, which is a difficult, risky, and expensive process [22]. Scientists think quantum computers can help us understand medications and how they affect people. As a result, pharmaceutical businesses can end up saving a tonne of time and money [23]. Companies could be able to find new medicinal remedies by doing further medication discoveries, leading to a more efficient pharmaceutical business, thanks to these developments in computing.

IV. Integration of AI and Quantum Computing in Cyber Defense

Improving cyber defences through synergistic integration is the focus here [24]. Modern cybersecurity threats can be effectively addressed by leveraging AI's data analysis, anomaly detection, and predictive analytics capabilities in tandem with quantum computing's capacity to resolve intricate cryptographic issues.

A. *AI- Enhanced Quantum Computing*

Cybersecurity, and encryption in particular, appears to gain a great deal from the introduction of quantum computing. The underlying premise of conventional encryption techniques like RSA and ECC is that factoring large numbers is difficult. The security of encrypted data is jeopardized since quantum computers may efficiently factor big numbers using techniques like Shor's algorithm (NIST to Standardize Cryptography Methods That Could Fight Quantum Computer Attacks, 2023) [25]. Cybersecurity researchers have been hard at work on post-quantum cryptography techniques to ward off assaults based on quantum computing in light of this danger. Numerous encryption methods, such as code-based, multivariate, and lattice-based cryptography, fall under the umbrella of post-quantum cryptography. Traditional cryptography systems are less vulnerable to quantum-based assaults because these methods can resist the processing capacity of quantum computers [26]. Data transmission between parties is guaranteed to be impenetrably secure thanks to algorithms based on AI that can maintain and optimize these quantum keys. The adoption of post-quantum cryptography methods is anticipated to improve cybersecurity by providing strong defenses against possible quantum computing threats.

B. *Quantum Machine Learning for Cyber- Security*

Quantum technologies are significant in the realm of security because digital information can be vulnerable and can interact with other technologies in intriguing ways. Some people argue that being ahead of the curve in quantum technologies provides a significant strategic advantage, and not just that. In addition to helping the economy, this also helps politics. What this is all about is how quantum computing affects cryptography. With these tools, it can get to very important and huge amounts of data. This poses a significant threat to the existing technology system. The area of cryptography is used to protect communication and data systems from these threats.

- Quantum computing is already having a noticeable impact on cryptography and other aspects of cyber security. Modern conversations and data sent via the internet or stored in the cloud almost always use public key encryption. To safeguard data transmitted over the open internet, every single browser in use today incorporates the crucial public-key encryption. Public key encryption is commonly used by corporations to secure internal communications, data, and user access to connected devices.
- Cybersecurity refers to the practice of keeping computer systems and the data, programs, and hardware within them safe against intruders. These attacks provide a threat of injury or disruption by allowing unlawful use, which could expose sensitive information. The classical communications infrastructure of the CPS is protected using quantum encryption, which is impenetrable to quantum computers. Cyberattacks have been on the rise in tandem with the trend towards remote employment and overall digitalization. Cyberattacks, including espionage and sabotage, are more likely to target organizations that gather and retain sensitive data, such as intellectual property, regardless of their size or industry.
- The threat actor and their motivation are the driving forces behind every cyberattack. The goals of threat actors determine how they are categorized: nation-state actors are adversaries with a political motivation and a proximity to a nation state; hacktivists are threat actors with a financial motivation. Though ideology guides them, the lines between them are blurry due to the fact that certain nation-state threat actors also act for financial gain.

V. Literature Review

This section review of literature identifies the recent development of quantum machine learning in cybersecurity, presenting quantum-enhanced anomaly detection, intrusion detection, and authentication mechanisms as well as discussing the issues of noisy quantum device and the changing nature of cyber threats using novel, integrated and optimized quantum-classic solutions in multiple fields.

Farouk et al. (2025) explored the integration of various quantum components as potential solutions to enhance and achieve the security objectives of ZTWN in the long term. Furthermore, three different quantum ML algorithms have been investigated on two anomaly detection datasets; the achieved accuracies outperform the implemented classical. Secure and tamper-proof communication between ZTWN entities is ensured by the creation of quantum communication protocols and identity authentication that utilize quantum characteristics like entanglement and superposition [27].

Vijayalakshmi, Shalinie and Bharathi (2025) present QSVM for improving the detection of anomalies in network traffic using the NSL-KDD dataset. A number of kernel functions are used in this study, including the radial basis function (RBF), polynomial, linear, and sigmoid, to examine their influence on QSVM. The degree to which each kernel can draw decision boundaries is plotted, which offers an understanding of how well the paradigm performs in identifying networks anomalies. This application is also beneficial because quantum computing allows improving the shortcomings of involving ML in security, and this research may contribute to the efficiency of the techniques implemented to identify irregularities [28].

Kukliansky et al. (2024) The new possibilities of quantum ML innovation have introduced novel opportunities into the field of ML, which have already shown potential. However, regrettably, the current devices of the noisy quantum era at the intermediate scale pose challenges for applications in quantum computing. In this case, the objective is to optimize the performance of the quantum neural network (QNN) for intrusion detection, leveraging the existing constraints of quantum computing. The method involves the effective encoding of classical information, selecting a QNN classifier, and optimizing the method to achieve maximum efficiency using the current computing potential of quantum computers. It ends with the optimization of a multilayered QNN architecture to be used with intrusion detection systems [29].

Rao et al. (2024) consider cooperation between such technologies as a change of paradigm in cybersecurity strategies, as a more dynamic/smarter approach is necessary nowadays. However, with any innovation, certain emerging issues arise. The increased complexity of cyber threats is testing the use of traditional security measures. Adaptive and robust defence measures are necessary to fend off ransomware assaults, zero-day flaws, and advanced persistent threats (APTs). Contemporary systems' interdependence increases worries about supply chain intrusions and the possibility of cascade vulnerabilities. A comprehensive and cooperative strategy encompassing technology, politics, and education is needed to address these challenges [30].

Tripathi, Upadhyay and Soni (2023) computer field that utilizes quantum devices, which has the ability to significantly improve speed over traditional processing. QIP has been expanded to include AI and ML in what is known as QAI and QML. In contrast to conventional ML algorithms, which are good at identifying patterns in datasets, QML seeks to create algorithms that use both classical and quantum computers, with the former used for dataset management and the latter for algorithms that are special to quantum technologies [31].

Chamma et al. (2023) investigates the possible effects of quantum computing on several domains, such as healthcare, economics, cybersecurity, encryption, HPC, and hacking. Because to quantum computing's enormous improvements in processing capacity, new algorithms and computing approaches might be developed that were previously unimaginable with classical computing, thus causing a revolution in these domains [32].

Faruk et al. (2022) from a thorough examination, it is possible to draw both solutions and threats from quantum cybersecurity, which necessitates the synthesis of basic and fundamental research in the field. examined the most recent cutting-edge methods for cybersecurity and quantum computing and provide a comprehensive, illustrative explanation of each. Quantum computing poses the most unexpected cybersecurity risks, but its results imply that it can also be used to improve cybersecurity [33].

Table I provides an overview of the research done on quantum-enhanced cybersecurity that exhibit QML methods, protocols and mixed methods that enhance detection and resistance, with challenges of hardware, scalability, noise, and implementation in various fields.

TABLE I. SUMMARY ON THE ROLE OF AI AND QUANTUM COMPUTING IN THREAT DETECTION

References	Study On	Approaches	Key Findings	Challenges	Limitations
Farouk et al. (2025)	Quantum security in ZTWN (Zero Trust Wireless Network)	Integration of QML algorithms and quantum protocols (identity authentication, communication)	Quantum models outperformed classical ones in anomaly detection; protocols enhance ZTWN security	Implementation in real-world ZTWN environments	Scalability and hardware constraints
Vijayalakshmi et al. (2025)	Quantum SVM (QSVM) for anomaly detection	QSVM on the NSL-KDD dataset using several kernel functions (linear, polynomial, RBF, and sigmoid)	QSVM effectively detects anomalies; kernel function choice impacts performance	Kernel optimization and real-time application	Quantum kernel implementation on NISQ devices
Kukliansky et al. (2024)	QNN for intrusion detection	Classical feature encoding + multilayered QNN classifier	Optimized QNN architecture shows promise within NISQ constraints	Quantum decoherence and noise	Limited quantum resources and data encoding complexity
Rao et al. (2024)	Cybersecurity strategies with quantum integration	Addressing APTs, ransomware, and supply chain attacks with AI + quantum	Emphasizes adaptive and intelligent cybersecurity models	Evolving cyber threats and attack sophistication	Integration with legacy systems and policy alignment
Tripathi et al. (2023)	Quantum AI/ML (QAI/QML) applications	Hybrid approach using classical and quantum computing	QML offers speedups and new learning paradigms over classical ML	Data representation, algorithm design for QML	Quantum hardware readiness for large datasets
Chamma et al. (2023)	Broad impact of quantum computing	Survey on quantum in medicine, finance, cybersecurity, etc.	Quantum computing can revolutionize processing across sectors	Quantum-safe cryptography and ethical concerns	Domain-specific adoption challenges
Faruk et al. (2022)	Evaluate quantum cybersecurity systematically	Analysis of quantum threats and solutions	Quantum is both a disruptive threat and potential solution	Mitigating unintended quantum vulnerabilities	Lack of mature frameworks for defense

VI. CONCLUSION AND FUTURE WORK

Quantum computing and AI together might change the way protect their computers and other areas. While it has the potential to deliver promising developments in encryption, threat detection, and safe connection, but it also presents additional difficulties, particularly in the area of cryptographic security. Cybersecurity is not the only field where quantum computing can change financial modelling, logistics optimization, and weather forecasting by solving complicated problems more efficiently than traditional systems. However, universal adoption is hindered by hardware constraints, integration difficulties, and ethical concerns. To maximally leverage its potential, researchers, policymakers, and industry executives must work in collaboration. With the advancement of quantum technologies, their responsible utilization important in creating a safer and more efficient digital age. Future studies should focus on developing quantum-attack-resistant cryptography systems. Improving QML for security use cases, including intrusion detection and anomaly detection, is still important. Also, hybrid quantum classical model optimization will help with easy integration into current security models. Improvements in quantum hardware, error correction, and scalability are also necessary to enhance computational efficiency. In addition, interdisciplinary cooperation among industry leaders, policymakers, and researchers is imperative in developing ethical standards and regulatory mechanisms. While quantum computing is advancing, responsible and secure usage will be imperative to solving world cybersecurity issues.

REFERENCES

[1] A. H. Hussain, M. N. Hasan, N. U. Prince, M. M. Islam, S. Islam, and S. K. Hasan, "Enhancing cyber security using quantum computing and Artificial Intelligence: A review," *World J. Adv. Res. Rev.*, vol. 10, no. 3, pp. 448–456, Jun. 2021, doi: 10.30574/wjarr.2021.10.3.0196.

[2] S. Garg, "Predictive Analytics and Auto Remediation using Artificial Inteligence and Machine learning in Cloud Computing Operations," *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, vol. 7, no. 2, 2019.

[3] A. Mishra, "AI-Powered Cybersecurity Framework for Secure Data Transmission in IoT Network," *Int. J. Adv. Eng. Manag.*, vol. 7, no. 3, pp. 05–13, 2025.

[4] G. Maddali, "An Efficient Bio-Inspired Optimization Framework for Scalable Task Scheduling in Cloud Computing Environments," *Int. J. Curr. Eng. Technol.*, vol. 15, no. 3, pp. 229–238, 2025.

[5] S. Singh and D. Kumar, "Enhancing Cyber Security Using Quantum Computing and Artificial Intelligence: A Review," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, no. 3, pp. 2581–9429, Jun. 2024, doi: 10.48175/IJARSCT-18902.

[6] D. Patel, "The Role of AWS in Modern Cloud Architecture: Key Strategies for Scalable Deployment and Integration," *Asian J. Comput. Sci. Eng.*, vol. 9, no. 4, 2024, doi: 10.22377/ajcse.v9i04.215.

[7] V. Thangaraju, "Security Considerations in Multi-Cloud Environments with Seamless Integration: A Review of Best Practices and Emerging Threats," *Trans. Eng. Comput. Sci.*, vol. 12, no. 2, 2024.

[8] S. Ness, N. J. Shepherd, and T. R. Xuan, "Synergy Between AI and Robotics: A Comprehensive Integration," *Asian J. Res. Comput. Sci.*, vol. 16, no. 4, pp. 80–94, Sep. 2023, doi: 10.9734/ajrcos/2023/v16i4372.

[9] A. Mishra, "AI-Powered Cyber Threat Intelligence System for Predicting and Preventing Cyber Attacks," *Int. J. Adv. Eng. Manag.*, vol. 7, no. 02, pp. 873–892, 2025.

[10] T. Sowmya and E. A. M. Anita, "A comprehensive review of AI based intrusion detection system," *Meas. Sensors*, 2023, doi: 10.1016/j.measen.2023.100827.

[11] A. R. Duggasani, "Scalable and Optimized Load Balancing in Cloud Systems: Intelligent Nature-Inspired Evolutionary Approach," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 5, pp. 2153–2160, May 2025, doi: 10.38124/ijisrt/25may1290.

[12] V. Thangaraju, "Enhancing Web Application Performance and Security Using AI-Driven Anomaly Detection and Optimization Techniques," *Int. Res. J. Innov. Eng. Technol.*, vol. 9, no. 3, 2025, doi: 10.47001/IRJIET/2025.903027.

[13] N. K. Prajapati, "Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 520–528, Apr. 2025, doi: 10.48175/IJARSCT-25168.

[14] M. Binhammad, S. Alqaydi, A. Othman, and L. H. Abuljadayel, "The Role of AI in Cyber Security: Safeguarding Digital Identity," *J. Inf. Secur.*, vol. 15, no. 02, pp. 245–278, 2024, doi:

10.4236/jis.2024.152015.

[15] S. Singamsetty, "Fuzzy-Optimized Lightweight Cyber-Attack Detection For Secure Edge-Based IoT Networks," *J. Crit. Rev.*, vol. 6, no. 07, pp. 1028–1033, 2019, doi: 10.53555/jcr.v6:i7.13156.

[16] O. A. Ajala, C. A. Arinze, O. C. Ofodile, C. C. Okoye, and A. I. Daraojimba, "Exploring and reviewing the potential of quantum computing in enhancing cybersecurity encryption methods," *Magna Sci. Adv. Res. Rev.*, vol. 10, no. 1, pp. 321–329, Feb. 2024, doi: 10.30574/msarr.2024.10.1.0038.

[17] A. Sharma, "Serverless Cloud Computing for Efficient Retirement Benefit Calculations," *Int. J. Curr. Sci.*, vol. 12, no. 4, 2022.

[18] V. Singh, "Reinventing Business with Cloud Integration: The Cost - Effectiveness of Replacing Legacy Applications," *Int. J. Sci. Res.*, vol. 13, no. 8, pp. 1882–1887, 2024.

[19] R. A. Jowarder and S. Jahan, "Quantum computing in cyber security: Emerging threats, mitigation strategies, and future implications for data protection," *World J. Adv. Eng. Technol. Sci.*, vol. 13, no. 1, pp. 330–339, Sep. 2024, doi: 10.30574/wjaets.2024.13.1.0421.

[20] V. Prajapati, "Enhancing Threat Intelligence and Cyber Defense through Big Data Analytics : A Review Study," *J. Glob. Res. Math. Arch.*, vol. 12, no. 4, pp. 1–6, 2025.

[21] S. S. Synam Neeli, "Critical Cybersecurity Strategies for Database Protection Against Cyber Attacks," *J. Artif. Intell. Mach. Learn. Data Sci.*, vol. 1, no. 1, pp. 2102–2106, Nov. 2022, doi: 10.51219/JAIMLD/sethu-sesha-synam-neeli/461.

[22] N. Patel, "AI-Powered Intrusion Detection and Prevention Systems in 5G Networks," in *2024 9th International Conference on Communication and Electronics Systems (ICCES)*, IEEE, Dec. 2024, pp. 834–841. doi: 10.1109/ICCES63552.2024.10859892.

[23] N. Jha, "Short Review on Quantum Computing and It Future Trends," *Ijres.Org*, vol. 9, no. 7, pp. 71–75, 2021.

[24] L. Thirupathi, B. Akshaya, P. C. Reddy, S. S. Harsha, and E. S. Reddy, "Integration of AI and Quantum Computing in Cyber Security," 2024, pp. 29–56. doi: 10.4018/979-8-3693-7076-6.ch002.

[25] S. B. Shah, "Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure," *J. Glob. Res. Electron. Commun.*, vol. 2, no. 2, pp. 01–07, 2025, doi: 10.5281/zenodo.14955016.

[26] M. Mozaffari-Kermani, R. Azarderakhsh, and A. Aghaie, "Fault Detection Architectures for Post-Quantum Cryptographic Stateless Hash-Based Secure Signatures Benchmarked on ASIC," *ACM Trans. Embed. Comput. Syst.*, vol. 16, no. 2, pp. 1–19, May 2017, doi: 10.1145/2930664.

[27] A. Farouk, S. Al-Kuwari, H. Abulkasim, S. Mumtaz, M. Adil, and H. H. Song, "Quantum Computing: A Tool for Zero-Trust Wireless Networks," *IEEE Netw.*, vol. 39, no. 1, pp. 140–148, Jan. 2025, doi: 10.1109/MNET.2024.3420166.

[28] M. Vijayalakshmi, S. M. Shalinie, and J. V. Bharathi, "A Comparative Analysis of Kernel Methods in Quantum Support Vector Machines for Network Anomaly Detection," in *2025 Fourth International Conference on Power, Control and Computing Technologies (ICPC2T)*, 2025, pp. 1–6. doi: 10.1109/ICPC2T63847.2025.10958729.

[29] A. Kukliansky, M. Orescanin, C. Bollmann, and T. Huffmire, "Network Anomaly Detection Using Quantum Neural Networks on Noisy Quantum Computers," *IEEE Trans. Quantum Eng.*, vol. 5, pp. 1–11, 2024, doi: 10.1109/TQE.2024.3359574.

[30] C. V. G. Rao, N. M. A. Chisty, S. K. Mishra, M. Sathe, S. Rizvi, and M. Soni, "Innovations, Difficulties, and Approaches for Next-Generation Cybersecurity: Protecting the Digital Future," in *2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies*, IEEE, Mar. 2024, pp. 1–6. doi: 10.1109/TQCEBT59414.2024.10545178.

[31] S. M. Tripathi, H. Upadhyay, and J. Soni, "Quantum Neural Network Classification-Based Cyber Threat Detection in Virtual Environment," in *2023 International Conference on Computational Science and Computational Intelligence (CSCI)*, IEEE, Dec. 2023, pp. 391–396. doi: 10.1109/CSCI62032.2023.00070.

[32] E. Chamma, A. McGee, A. Gillmann, I. McNallan, and M. Mahmoud, "Feasible Applications of Quantum Computing in Varying Fields," in *2023 International Conference on Computational Science and Computational Intelligence (CSCI)*, IEEE, Dec. 2023, pp. 454–459. doi: 10.1109/CSCI62032.2023.00080.

[33] M. J. H. Faruk, S. Tahora, M. Tasnim, H. Shahriar, and N. Sakib, "A Review of Quantum Cybersecurity: Threats, Risks and Opportunities," in *2022 1st International Conference on AI in Cybersecurity (ICAIC)*, IEEE, May 2022, pp. 1–8. doi: 10.1109/ICAIC53980.2022.9896970.

