International Journal of Applied Mathematics
Volume 38 No. 8s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

FUTURE-PROOFING SECURITY: A COMPREHENSIVE SURVEY ON GENERATIVE AI AND QUANTUM INNOVATIONS IN CYBER DEFENSE

Dr. Aniket Deshpande

Researcher, Department of Computer Science and Engineering, Sunrise University, Alwar, India

Email id : anik.deshpande@gmail.com

Abstract

In the contemporary digital landscape, cyber security has become a paramount concern, with organization increasingly exposed to a wide array of sophisticated cyber threats. Traditional security measures, while foundational are often inadequate in combating the evolving tactics employed cyber criminals, especially those leveraging advanced technologies like Artificial Intelligence (AI) and Machine Learning (ML). The rise of generative AI and quantum computing represent a paradigm shift in how cyber defense strategies can evolve to address these complex challenges. This review explores the integration of generative AI and quantum innovations in enhancing cyber security frameworks. Conventional studies highlight the significant role of AI in automating threat detection, vulnerability identification, and response optimization. However, challenges remain, such as the interpretability and transparency of AI models, biases in training data, and concerns about over reliance on automated systems. Furthermore, the advent of quantum computing poses a unique challenge to traditional encryption techniques, requiring the development of quantum resistant security protocols. This paper done comprehensive examination of how generative AI and quantum computing can collaborate to create adaptive, intelligent, and future-proof security systems. By synthesizing current advancements, this review aims to provide a holistic accepting of the convergence between these technologies and their potential to transform cyber defense. The review also discusses the challenges of implementing these technologies, particularly focusing on data integrity, model transparency, and the integration of quantum-safe encryption. Ultimately, this paper contributes to the ongoing discourse on next-generation cyber security solutions, offering insights into the synergy between AI and quantum technologies for resilient and dynamic defenses.

Keywords: Generative AI, Quantum Computing, AI driven security, cyber-attacks, cyber security, AI, ML, defense.

1. Introduction

In the modern digital landscape, cyber security has emerged as a crucial field keen to protecting computer systems, networks, and sensitive data from a numerous of cyber threats. As organizations increasingly rely on digital technologies for their operations, the potential for cyber-attacks has escalated significantly [1]. Cyber security encompasses a wide array of practices and technologies designed to secure against unauthorized access, data breaches, and other malicious activities aimed at disrupting normal business operations. The growing

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

complexity of these threats necessitates a robust cyber security framework that combines people, processes, and technology to create a comprehensive defense strategy. The significance of cyber security dates back to the 1970s when early computer networks began to emerge. As these networks expanded, so did the vulnerabilities that malicious individuals could exploit. The evolution of cyber security has been fuelled by the necessity to protect critical information and ensure the reliability of systems. Today, cyber security consists of various components, such as application security, network security, data protection, and incident response. Organizations employ multiple layers of security measures to fortify their defenses against cyber threats [2].

Widespread cyber security methods include firewalls, Intrusion Detection Systems (IDS), encryption protocols, and Multi-Factor Authentication (MFA) [3]. Firewalls act as the primary line of defense by monitoring network traffic based on predefined security rules to prevent unauthorized access. They serve as a barrier between trusted internal networks and untrusted external networks, filtering incoming and outgoing traffic to block malicious attempts [4]. Intrusion Detection Systems analyze network activity for any suspicious behaviour and alert administrators of potential breaches. These systems can be configured to detect anomalies in real-time, thereby enabling swift responses to likely threats [5]. Encryption protocols safeguard sensitive data by converting it into an unreadable format that only authorized users can decipher. This process ensures that even if data is intercepted during transmission or accessed without permission, it remains secure from unauthorized viewing. Multi-Factor Authentication enhances security by requiring users to provide multiple verification factors before accessing sensitive systems. By combining something the user knows like a password with something they have like a smartphone, MFA significantly reduces the likelihood of unauthorized access.

While traditional techniques have proven effective in the past, they often fall short when it comes to dealing with sophisticated cyber threats that are constantly evolving [6]. Cybercriminals are now using advanced tactics like Artificial Intelligence (AI) and Machine Learning (ML) to bypass traditional security measures, emphasizing the need for more adaptive and intelligent solutions that can evolve with emerging threats [7]. The rise of automated attacks powered by AI has highlighted vulnerabilities in existing systems, making it imperative for organizations to rethink their cyber security strategies [8]. Generative AI has merged as a critical assets in improving cyber security initiatives. Through the use of ML algorithm to generate new content derived from existing data patterns organization are able to establish adaptive security systems that learns from past incident and adjust to avert future threats. For instance, generative models can simulate potential attack scenarios, enabling security teams to proactively identify weaknesses in their defenses and implement necessary countermeasures. This capability not only improves the overall resilience of security systems but also enables quick responses to emerging threats.

Moreover, generative AI can automate threat detection and response processes significantly reducing the time needed to neutralize threats while minimizing potential damage [9]. AI-driven systems can analyze large amounts of data in real-time, detecting anomalies and potential breaches more efficiently than traditional methods. This enhanced capability allows

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

organizations to respond swiftly to incidents and allocate resources more effectively based on real-time insights. In spite of its benefits, generative AI in cyber security has its limitations. Dependency on AI models raises concerns about interpretability and transparency, making it difficult for security professionals to trust automated responses during critical incidents. If an AI system makes an erroneous decision or misidentifies a threat due to a lack of contextual understanding, it could lead to severe consequences for an organization security posture. Additionally, generative AI models require high quality training data to function effectively; biases present in this data could lead to skewed results or misidentifications [10].

In light of these challenges, there is a growing interest in integrating quantum computing with generative AI to enhance cyber security further. Quantum computing introduces a new paradigm for processing information through qubits that can exist in multiple states simultaneously. This capability enables quantum computers to perform complex calculations at unprecedented speeds, potentially revolutionizing cryptography and data encryption methods. As traditional encryption techniques become increasingly vulnerable to quantum attacks wherein quantum computers could decipher encrypted data in mere moments organizations must adapt by developing quantum-resistant encryption algorithms. The urgency for such adaptations is underscored by the impending reality that quantum computing will soon be capable of breaking conventional encryption standards that have long been relied upon for securing sensitive information.

The convergence of generative AI and quantum computing holds immense promise for enhancing cyber security measures. For instance, generative AI can assist in designing robust quantum encryption protocols by analyzing vast datasets to identify patterns that could inform the development of more secure algorithms [11]. This collaboration may lead not only to stronger encryption methods but also to improved efficiency in how these algorithms are implemented across various platforms. Additionally, quantum computing ability to process large amounts of data rapidly can facilitate real-time threat analysis and response coordination across interconnected systems. This synergy extends beyond encryption; it encompasses various aspects of cyber security operations. Generative AI can optimize quantum algorithms for specific tasks, improving their efficiency and effectiveness in real-world applications [12].

While traditional cyber security techniques have laid a strong foundation for protecting digital assets, the integration of generative AI and quantum computing represents a significant advancement in addressing modern cyber threats. By leveraging these technologies together through enhanced automation capabilities provided by generative AI alongside the computational power offered by quantum computing organizations can create a more resilient defense strategy capable of adapting to an ever-evolving threat landscape. This integration not only enhances existing security measures but also paves the way for innovative solutions that can anticipate and neutralize emerging threats before they materialize. As we move forward into an increasingly complex digital future, embracing this synergy will be crucial for maintaining robust cyber defenses that protect sensitive information and ensure operational integrity against sophisticated adversaries.

Received: August 09,2025

International Journal of Applied Mathematics
Volume 38 No. 8s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Furthermore, integrating generative AI with quantum computing can enhance incident response strategies by automating decision-making processes based on real-time threat intelligence gathered from multiple sources. This capability allows organizations not only to react more quickly but also to anticipate potential attacks before they occur. This paper will delve into several key areas: the current state of generative AI applications in cyber security; an overview of quantum computing advancements relevant to cyber defense; case studies illustrating successful implementations; challenges faced by organizations adopting these technologies; and future directions for research and development in this critical field. By synthesizing insights from various sources and perspectives, this paper aims to provide a holistic understanding of how generative AI and quantum innovations can collectively contribute to future-proofing cyber security strategies.

- To examine the existing cyber security frameworks, techniques, and methodologies to understand their effectiveness against evolving cyber threats.
- To investigate how generative AI can enhance cyber security measures by enabling security systems that learn from past incident and proactively identify vulnerabilities.
- To discuss the challenges associated with implementing generative AI in cyber security, including issues related to interpretability, transparency, and the quality of training data.
- To develop a framework that combines generative AI and quantum computing to enhance organizational resilience against sophisticated cyber threats.

2. Survey Methodology

Different methods are used for fetching the suitable content. Some of the methods includes fetching the content probing different Database (DB) and scrutinizing the references with specific criteria. Figure 1. Depicts the

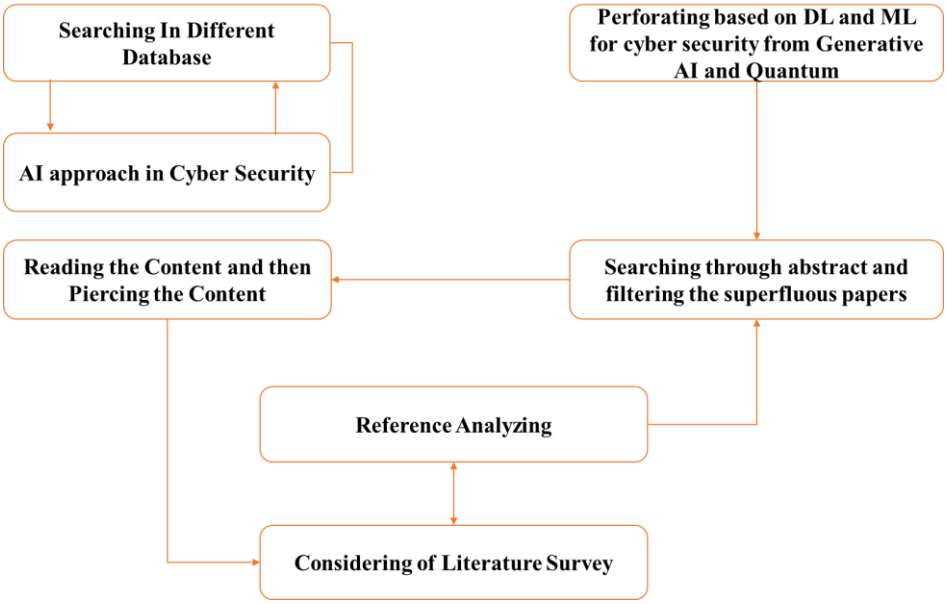

Figure 1. Survey Methodology

Searching Database

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Searching content related to cyber defense ad detection using AI techniques in different DB. Along with cyber security in Generative AI and Quantum computing. Key term used for searching the content including “Generative AI in cyber security”, “Quantum computing in cyber defense”, “AI-driven threat detection”, “Traditional cyber security methods”, and “Synergy between Generative AI and Quantum Computing”.

Content Fetching

During the Preliminary screening, studies were selected based on their relevance to generative AI and Quantum Computing within the context of cyber security. Abstract were meticulously reviewed to ensure alignment with the focus of this survey. Paper from IEEE, springer, Wiley, Scopus, Tailor an Francis, Web of science, Science Direct, PubMed, MDPI, NCI, ACM are also considered for fetching the content.

Reference Analysis

A total of 60 papers published between 2021 and 2024 were included for review. These papers provided insights into several of generative AI and quantum innovation in cyber security, focusing on their applicability in threats detection, intrusion prevention, and overall cyber defense strategies.

Inclusion Criteria

- Articles specifically addressing the intersection of generative AI and Quantum computing in cyber security were selected.
- Only peer-reviewed paper published between 2021 and 2024 were considered.
- Studies emphasizing innovative techniques for threat detection and cyber defense were prioritized.

Exclusion Criteria

The following criteria were applied to exclude irrelevant studies:

- Papers with unclear titles or abstracts that did not focus on generative AI or quantum computing in cyber security were omitted.
- Non-English publications were excluded to maintain consistency in analysis.
- Research lacking a clear aim or methodology was disregarded.
- Duplicates or papers reporting similar research findings without novel contributions were not considered.

3. Significance of Generative AI and Quantum Computing in Cyber security

The rapid advancement in Generative AI and Quantum Computing are significantly shaping the cyber security landscape. Together, these technologies promise both transformative capabilities and new challenges, particularly, in enhancing defense mechanism, security data, and addressing vulnerabilities posed by increasingly sophisticated cyber threats.

Generative AI in Cyber Security

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Generative AI, which includes advanced model such as Generative Adversarial Networks (GANs), transformer base models like GPT, and either Deep Learning (DL) techniques, has emerged as a powerful tool in cyber security for both offensive and defensive applications. There are some key areas in generative AI is making an impact, such as enhancing threats detection and simulation , the simulating realistic cyber-attacks and testing the resilience of security systems [13]. These AI model can generate synthetic attack data, which is crucial for training ML model for Intrusion Detection (ID) and improving cyber security protocols. Generative AI has been successfully used in generating adversarial examples that mimic new forms of malware and exploits, allowing defenders to prepare against previously unseen threats. This approach is especially useful in identifying vulnerability in ML model that could exploited by attackers. Similarly, Generative AI has significantly transformed the landscape of cyber security by enabling the development of adaptive defense systems, particularly through intelligent firewalls. Unlike traditional firewalls, which rely on static, rule-based configurations, intelligent firewalls leverage generative AI to learn and evolve in response to emerging attack patterns. Research conducted by Gupta et al. (2023) illustrates that AI-driven systems can autonomously adjust firewall rules by analyzing current network traffic and generating new defense strategies. This capability allows for continuous updates to security protocols based on real-time threat analysis, enhancing the overall network security posture. The dynamic adaptability of these systems not only improves detection rates but also provides context-aware protections, making them more resilient against advanced evasion tactics employed by cyber adversaries [14].

In addition to enhancing defensive measures, generative models play a crucial role in automated malware generation and analysis. These models can create synthetic variants of known malware, which are essential for testing the efficacy of antivirus software and intrusion detection systems. This is particularly relevant in combating polymorphic and metamorphic malware that continuously evolves to evade signature-based detection methods. The research highlights the application of Generative Adversarial Networks (GANs) in producing new malware variants, offering critical insights into how detection systems can be improved. By simulating diverse attack scenarios, cyber security teams can better understand potential threats and refine their defenses, ultimately leading to more robust security solutions that pre-emptively address emerging vulnerabilities before they can inflict damage.

Quantum Computing in Cyber Security

Quantum computing has the ability to completely transform cyber security by offering more robust encryption techniques while also posing a threat to the security of current cryptographic systems. Recent advancements showcase the following significant effects, Quantum computing poses a significant threat to traditional encryption methods like RSA and ECC because it can solve problems much faster than classical computers. This highlights the importance of quantum cryptography for securing data in the future. One effective technique in quantum cryptography is Quantum Key Distribution (QKD), which can detect any eavesdropping on communication channels in real-time. A study [15], by Radanliev et al. (2023) showed how combining the BB84 protocol with NIST-approved quantum-resistant

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

algorithms offers strong encryption protection against quantum attacks. These developments are essential for safeguarding sensitive communications in the age of quantum computing.

Quantum computing is a major threat to traditional cryptography due to the potential of algorithms like Shor's Algorithm to factor large numbers quickly [16]. This has led to concerns about the security of current cryptographic systems and has spurred research into post-quantum cryptography [17]. The National Institute of Standards and Technology (NIST) has been working on developing quantum-resistant encryption protocols to secure communications and data storage in the face of quantum threats. On the other hand, quantum computing has the potential to greatly improve ML applications in cyber security. Quantum-enhanced ML can significantly enhance the speed and efficiency of algorithms used for anomaly detection and threat analysis [18]. Studies have shown that quantum computers have the ability to process large amounts of data quickly, making it easier to identify patterns and anomalies that signal potential cyber threats. Recent research has also demonstrated that quantum ML algorithms can improve the accuracy and speed of detecting malware and intrusion attempts, leading to faster responses to security breaches. The progress in both areas highlights how quantum computing is both a challenge to current cryptographic methods and a powerful tool for strengthening cyber security defenses.

4. Conventional Cyber security Methods

Traditional cyber security practices have played a crucial role in defending digital systems from diverse cyber threats. These practices consist of different tools and strategies aimed at securing systems, networks, and information from unauthorized intrusion, theft, and harm. While conventional cyber security methods have been improved and honed over time, they are facing more challenges as cyber threats become more sophisticated and abundant. This study evaluates key traditional cyber security approaches, emphasizing their efficacy and difficulties based on current research.

Firewalls are commonly used security mechanisms in traditional cyber security, serving as barriers that control and monitor traffic between trusted internal networks and untrusted external networks. They enforce predefined security rules regarding IP addresses, ports, and protocols. Different types of firewalls include packet-filtering firewalls, stateful inspection firewalls, proxy firewalls, and Next-Generation Firewalls (NGFWs) that offer advanced features like intrusion prevention and application awareness. Despite their ability to filter known threats, firewalls have limitations such as difficulty in detecting unknown attacks, incapacity to adapt to emerging threats in real-time, and susceptibility to bypass techniques used by attackers [19].

Intrusion Detection and Prevention Systems (IDPS) play a critical role in traditional cyber security by identifying and responding to suspicious activities in networks or systems. These systems consist of Intrusion Detection Systems (IDS) [20], that alert administrators about potential threats and Intrusion Prevention Systems (IPS) that actively block malicious activities. IDPS can be categorized as Network-based IDS (NIDS), host-based IDS (HIDS), signature-based detection systems, and anomaly-based detection systems. However, IDPS

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

encounter challenges like high rates of false positives and negatives, scalability issues in complex networks, and reliance on batch processing hindering real-time threat mitigation [21].

Antivirus and anti-malware software are essential components of traditional cyber security strategies, aimed to detect, prevent, and eliminate malicious software through signature-based detection, heuristic analysis, and behavioural analysis. Despite their common use, these tools have drawbacks such as inability to detect zero-day attacks, resource-intensive deep scans causing system slowdowns, and vulnerability to evasion techniques utilized by malware developers [22].

Encryption serves as a cornerstone of data protection by converting plaintext into unreadable formats to ensure confidentiality and integrity during digital communications [23]. It encompasses symmetric encryption using the same key of decryption and encryption, asymmetric encryption utilizing public-private key pairs, and hybrid encryption that combines both methods. Nevertheless, encryption is not without limitations; it faces vulnerabilities from quantum computing attacks capable of breaking traditional methods like RSA through algorithms such as Shor's algorithm. Moreover, key management remains a critical challenge; improper handling can lead to significant vulnerabilities. Furthermore, the performance overhead associated with encryption processes can introduce latency issues affecting system performance. The several studies emphasizing the critical importance of cyber security measure in today's digital landscape. The study [24], examines automated intrusion detection, highlighting a classifier developed using the NSL-KDD dataset that achieved 79.1% accuracy with the J48 tree and improved to 82.0% through Random Projection with the PART algorithm. The review [25], also explores AI driven solutions for real time threat detection, focusing on ML and NLP to identify anomalies and phishing attempts while advocating for human oversight in cyber security frameworks. Additionally [26], it addresses challenges in Cyber Physical Systems (CPSs) by proposing tailored intrusion detection mechanisms and underscores the significance of encryption strength, firewall configuration, and authentication protocols in protecting e-commerce platforms against cyber threats. Ultimately, the study [27] advocates for a layered security approach that integrates firewalls, Intrusion Detection Systems (IDPS), encryption, and MFA to effectively protection sensitive information from increasingly sophisticated cyber threats [28].

While conventional cyber security methods such as firewall, IDPs, antivirus software, and encryption have been foundational in protecting systems and data, they face significant challenges in addressing modern, sophisticated cyber threats. These methods are largely static, relying on predefined rules and signature that can be easily bypassed or evaded by advanced attacks, such as zero day exploits, polymorphic malware, and insider threats. Additionally, the growing complexity and volume of cyber-attacks, along with the increasing reliance on could computing and IoT, further strain the efficacy of traditional security measures. In contrast, AI driven cyber security methods offer dynamic adaptive, and more effective solutions to these challenges. ML and DL enables the real time threats detection and response by learning from past incidents and identifying emerging attack patterns [29].

5. AI Techniques in Cyber security

Received: August 09,2025

International Journal of Applied Mathematics
Volume 38 No. 8s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

AI has emerged as a transformative force in cyber security, offering new ways to detect, prevent, and mitigate cyber threats. AI, enables dynamic, adaptive, and scalable security measures that can continuously learn from data and adapt to new threats. This section explores the AI techniques currently applied in cyber security, based on recent research and developments.

ML in Cyber Security

ML a subset of AI, has found extensive use in cyber security for automating threats detection, anomaly detection, and classification tasks. ML algorithms study from historical information, identifying patterns and making predictions based on that learning [30].

The supervised learning techniques are commonly used to training model on labelled datasets, such as benign or malicious network traffic or known malware signatures. Algorithms like decision tree, support vectors machines (SVM), and Random Forests (RF) [31] are widely employed to classify data into predefined categories. For example, SVM can distinguish between malicious and legitimate network traffic, helping to automate the identification of intrusion attempts [32]. And unsupervised learning techniques such as K-means clustering, auto encoders, and isolation forest, are used to identify anomalies in data without requiring labelled training sets [33]. These models works by learning the normal patterns in system or network behaviour and flagging deviations as potential threats. This is particularly useful for detecting zero day attacks or malware strains that do not match known signatures. Auto-encoders a type of Neural Network (NN), have proven effective in identifying network instruction by reconstructing inputs data and highlights outliers as potential anomalies. Similarly, Reinforcement Learning (RL) is increasingly being explored for cyber security applications such as adaptive firewalls, dynamic threat intelligence systems, and real-time response strategies [34]. In reinforcement learning, an agent learns to make decisions by interacting with its environment and receiving feedback in the form of rewards or penalties. The model adapts its actions to maximize the cumulative reward over time. RL can be used to automatically adjust security configurations or firewall rules based on evolving attack patterns and detected vulnerabilities.

DL for Advanced Threat Detection

DL, a more advanced subset of ML utilized multi layered NN to automatically extract high-level features from raw data. DL models have shown great promise in tackling complex cyber security tasks, including malware detection, ID and network traffic analysis [35].

CNN are widely used in mage and pattern recognition tasks, but recent research has extended their use to malware detection [36]. By converting binary files or network traffic into image like structure CNN can automatically learn the relevant features that distinguish malicious files from benign ones [37]. The study [38] addressed the increasing frequency and severity of cyber-attacks on the rapidly evolving Internet of Things (IoT), emphasizing the need for effective detection methods for malicious attacks like botnets. It employs a hybrid DL approach, specifically the CNN-LSTM technique, to enhance botnet detection, leveraging natural language processing alongside convolutional and long short-term memory networks to

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

capture spatial correlations and long-term dependencies in data. The results demonstrate that the proposed CNN-LSTM model achieves an impressive detection accuracy of 99.19%, significantly outperforming traditional methods such as decision trees 98% and support vector machines 95%, thereby providing a robust solution for improving security in IoT environments against sophisticated malware threats. Similarly, study have demonstrate the effectiveness of CNNs in identifying polymorphic malware, that change its code to evade detection by traditional signature based model [39].

Natural Language Processing (NLP) is a branch of AI that focuses on how computers interact with human language. It has become increasingly important in identifying phishing attacks, social engineering tactics, and malicious email content. Various studies have shown the effectiveness of using NLP techniques, especially in classifying text for detecting phishing emails [40]. Researchers have used methods like text classification and Named Entity Recognition (NER) to analyze the language and identify suspicious patterns in emails to determine if they are benign or malicious. One study introduced a new machine learning framework that utilized NLP techniques to accurately detect phishing emails with a precision of 99.97% and an F-score of 99.98%. Additionally, sentiment analysis has become a crucial aspect of NLP that can recognize manipulative language or emotional triggers commonly used in social engineering attacks. AI models can analyze the tone and urgency of messages to flag suspicious content, particularly in spear-phishing situations where attackers create personalized messages [41]. Overall, advancements in NLP have significantly improved the detection of phishing attacks, surpassing traditional rule-based methods, which underlines the importance of continuous innovation in cyber security strategies.

5.1. Generative AI and Its Impact on Cyber Security

Generative AI plays a significant role in enhancing cyber security by utilizing advanced neural networks like Variation Auto-encoders (VAEs) and Generative Adversarial Networks (GANs) to dynamically generate and analyze data. Unlike traditional AI, which depends on fixed models and predefined regulations, generative AI has the capability to simulate different cyber-attack scenarios for proactive threat detection and response. Its capacity to learn autonomously from diverse datasets enables continuous adaptation to evolving threats, enhancing anomaly detection and malware analysis. Moreover, generative AI automates regular cyber security tasks, reducing the risk of human error and allowing professionals to concentrate on complex issues. In general, generative AI provides a more dynamic and effective strategy for addressing sophisticated cyber threats compared to traditional methods [42].

Threat Detection

Generative AI models, particularly GANs, have been effectively utilized to simulate diverse cyber-attacks. By training on synthetic data that mirrors real-world attack patterns, these models empower cyber security systems to proactively identify and respond to emerging threats. Research has shown that generative models can significantly enhance the detection capabilities of security systems by providing a more comprehensive understanding of potential attack vectors. Similarly auto encoder are employed to detect unusual behaviour in network

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

traffic or user activities. By reconstructing normal patterns, these models can identify deviations that may indicate potential threats. This approach allows organizations to maintain a baseline of expected behaviour and quickly flag anomalies that could signify security incidents. Similarly, Generative models are instrumental in generating malware samples for analysis, thereby improving antivirus programs effectiveness. Techniques such as GAN-based augmentation create diverse datasets that enhance the training of cyber security systems, enabling them to recognize and mitigate a broader range of malware threats [43].

Defensive Counter Measures

Recent research emphasizes the significant impact of generative AI techniques on improving cyber security measures. Defensive Generative Adversarial Networks (D-GANs) have proven to be effective in refining decision boundaries within machine learning systems, thereby enhancing their ability to defend against adversarial attacks and boosting classifier resilience against complex threats. Generative AI also plays a crucial role in generating synthetic data, which helps overcome the limitations of scarce labelled data and enables the creation of diverse datasets necessary for training accurate and robust cyber security models. As well as prevailing study from CETaS highlights the dual functionality of generative AI in cyber security, acknowledging its potential to both develop malicious software and strengthen defensive strategies. Despite concerns surrounding its potential use in creating new threats, it is widely agreed that generative AI mainly automates existing malicious tactics rather than independently generating sophisticated malware. Moreover, studies suggest that generative AI can automate the detection and exploitation of software vulnerabilities, providing cyber security experts with advanced tools to navigate intricate threat landscapes. The incorporation of generative AI into conventional security frameworks represents a meaningful advancement in defense strategies, offering innovative solutions to modern cyber security challenges.

Generative Data Encryption and Decryption

Recent research has highlighted the crucial importance of generative AI in the advancement of cryptographic techniques, especially in the realm of data encryption and decryption. One notable example is the creation of Crypto-Gen-Sec, a hybrid algorithm that merges GANs with RL to strengthen cryptographic defenses against evolving cyber threats. This algorithm can simulate various attack scenarios, allowing for real-time adjustments and improving threat detection and response times significantly, showing a 20% speed boost and a 25% increase in resilience compared to traditional methods [44].

Moreover, studies have pointed out the significance of integrating homomorphism encryption and differential privacy into generative AI frameworks to protect sensitive data during computations. Homomorphism encryption enables operations to be carried out on encrypted data without decryption, ensuring confidentiality while enabling risk assessments and compliance with regulations like DORA in the finance sector. Differential privacy further heightens security by ensuring that the results from generative AI models do not reveal individual data points from training datasets, thus safeguarding user privacy. Furthermore, research has explored the potential of generative AI in designing advanced encryption

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

algorithms that are customized for specific data types and communication channels. These advancements not only enhance security but also boost efficiency, addressing the computational obstacles posed by traditional encryption methods. As generative AI progresses, its use in cryptography is anticipated to play a significant role in strengthening data security against increasingly sophisticated cyber threats.

5.2. Generative AI in Threat Detection and Response

Recent research has delved deeper into the potential of generative AI to improve threat detection and response in cyber security. A significant advancement is seen in the use of generative AI to automate safety measures and streamline the implementation of cyber defense protocols. This automation allows generative AI to analyze incidents in real-time, prioritize threats based on severity, and create response playbooks with automated countermeasures. By responding quickly, this technology reduces the window of opportunity for attackers and strengthens organizational defenses. Similarly, Generative AI has also been employed in malware analysis by generating artificial malware samples that mimic known attack methods. This helps cyber security professionals understand how these samples interact with systems and exploit vulnerabilities in a secure sandbox environment. By studying these behaviours, researchers gain valuable insights into the tactics used by cybercriminals and improve their understanding of emerging threats [45].

Another innovative use of generative AI is in creating patches for vulnerabilities. When critical vulnerabilities are identified, generative AI can analyze the problem, create customized patches, and test them in a controlled setting. This automation saves time and effort in addressing security weaknesses, allowing organizations to enhance their security posture and reduce the risk of exploitation by threat actors. Moreover, IBMs introduction of a generative AI-powered Cyber security Assistant demonstrates practical applications of this technology in threat detection and response services [46]. This assistant speeds up the identification and investigation of security threats by using historical correlation analysis to cross-reference alerts from various sources like SIEM, network telemetry, and endpoint detection and response systems. The integration of generative AI has reportedly reduced alert investigation times by 48%, enabling security analysts to proactively respond to potential threats. Overall, these studies show that generative AI not only improves traditional threat detection methods but also offers innovative solutions to complex cyber security challenges [47]. By automating processes, generating synthetic data for analysis, and enhancing incident response capabilities, generative AI is set to play a crucial role in fortifying defenses against increasingly sophisticated cyber threats.

5.3. Application of Generative Models

Generative AI is revolutionizing cyber security by providing innovative solutions that enhance threat detection, response, and overall security posture. Its applications span various domains within cyber security, making it a vital tool for modern defense strategies.

Advanced Threat Intelligence

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

One of the primary application of generative AI is in threat intelligence, where it analyses vast amount of historical cyber security data to identify patterns and predict future threats. By leveraging ML algorithms, generative AI models can continuously learn from new data, allowing administrations to anticipate and mitigate risks before they materialize. This practical approach enhances the ability to stay ahead of cybercriminals by swiftly adapting to their tactics [48].

Anomaly Detection

Generative AI significantly improves anomaly detection by establishing baselines of normal behaviour within network traffic and user activities. By flagging deviations from these baselines, it can identify potential security incidents that traditional systems may overlook. This capability is crucial for detecting zero day attacks and other sophisticated threats that require immediate attention [49].

Automating Security Tasks

Another significant application is in the automation of security tasks such as incident response and patch management. Generative AI can quickly analyze vulnerabilities in codebases, suggest appropriate patches, and even apply them automatically. This streamlining of processes reduces the workload on cyber safety teams, allowing to focus on more difficult challenges while enhancing the overall efficiency of security operations [50].

Phishing Prevention

Generative AI enhances phishing prevention efforts by developing models that detect malicious emails through sophisticated language pattern analysis. By analyzing patterns in legitimate communications, generative AI can classify understated signs of phishing attempts that may otherwise go hidden, thereby protecting individuals and organizations from potentially devastating attacks [51].

Realistic Cyber-attack Simulations

In the realm of security training, generative AI can create realistic simulations of cyber-attacks. These immersive training scenarios help security teams improve their preparedness and decision-making skills in real-world situations. By simulating advanced attack scenarios, organizations can test their defenses against emerging threats and refine their incident response strategies [52].

Enhanced Security Automation

Generative AI also plays a pivotal role in enhancing security automation. By processing vast volumes of log data and correlating events, it can uncover hidden threats more efficiently than traditional methods. This capability allows for rapid adjustments to defenses in real-time, significantly improving response times compared to manual interventions [53].

5.4. Quantum Computing Applications in Cyber security

Quantum computing is a significant advancement in computing power that has important implication for cyber security. As quantum technologies progress, they offer better security

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

measures but also present challenges to current encryption systems. This part discusses the key concepts of quantum cryptography, the influence of quantum computing on standard encryption techniques, and the creations if improved security solutions using quantum technology [54].

Quantum cryptography uses quantum mechanics principles to protect communications from eavesdropping and cyber threats. An important application is QKD, which allows two parties to create a secure shared key resistant to eavesdropping. QKD utilizes quantum properties like superposition and entanglement to detect any attempts at intercepting the key exchange process [55]. This sets quantum cryptography apart from classical methods that rely on mathematical complexity for security. The contrast between classical and quantum cryptography is significant. Classical cryptographic systems rely on solving complex problems like factoring large numbers as in RSA or discrete logarithms (as in ECC), while quantum cryptography offers a different approach that can resist attacks from quantum computers. Quantum cryptography offers the potential to protect communications from future quantum-based attacks, ensuring that confidential information remains secure even in a post-quantum era [56].

5.4.1. Encryption an Decryption

Encryption and Decryption techniques in quantum cyber security are rapidly evolving leveraging the principle of quantum mechanism to address vulnerabilities posed by advancements in quantum computing. A key method is QKD, which allows two parties to securely generate a shared encryption key utilizing quantum bits, also known as qubits. In QKD, single photons are transmitted, and their quantum states are manipulated to create truly random keys that remain secure against eavesdropping. The fundamental principle behind QKD is that any attempt to observe the photons alters their state, thereby alerting the communicating parties to potential interference. This characteristic ensures that the integrity of the key exchange process is maintained, making it a cornerstone of quantum cryptographic systems.

Besides QKD, quantum cryptography utilizes various fundamental principle of quantum mechanism such as super position, entanglement, and the no cloning theorem. Superposition enables qubits to be in several states at once, greatly enhancing the complexity of any possible attacks. For example, while classical bits can only exist in binary states 0 or 1, qubits can represent both at the same time, similar to a dimmer switch that can be set to any brightness level from completely off to fully on. Entanglement creates a correlation between qubits such that a change in one instantaneously affects its entangled partner, regardless of distance. This property can be exploited for secure communication, ensuring that any alteration during transmission signals potential eavesdropping [57]. The no-cloning theorem further enhances security by preventing the perfect copying of quantum states, making it impossible for an eavesdropper to replicate the information without detection. Recent advancements in quantum cyber security also explore hybrid systems that integrate classical cryptographic methods with quantum techniques [58]. These hybrid approaches aim to provide robust security while addressing practical challenges such as distance limitations and implementation costs associated with purely quantum methods. For instance, organization are progressively urged to

Received: August 09,2025

International Journal of Applied Mathematics
Volume 38 No. 8s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

implement post quantum cryptographic algorithm tailored to resist assaults from both traditional and upcoming quantum computers. These algorithms generally depends on intricate mathematical framework through to withstand quantum assaults, thereby providing enduring data security.

Moreover, researchers are investigating the use of quantum repeaters, which can extend the range of QKD by overcoming distance limits inherent in photon transmission over fiber optic cables. Quantum repeaters work by purifying segments of noisy channels before connecting them, thus creating a secure communication line over longer distances. This capability is crucial for real-world applications where secure communication needs to span vast geographical areas. The integration of advanced encryption and decryption techniques grounded in quantum mechanics represents a significant evolution in cyber security strategies. These methods not only aim to protect data from current threats but also prepare for the impending challenges posed by powerful quantum computing capabilities. As research continues to advance in this field, the promise of unbreakable encryption through quantum technologies becomes increasingly tangible, positioning quantum cryptography as a vital component of future cyber security frameworks.

5.5. Synergy between Generative AI and Quantum Computing

The synergy between generative AI and Quantum computing in cyber security is a transformative frontier that promises to enhance threat detection, defense mechanism, and predictive analytics.

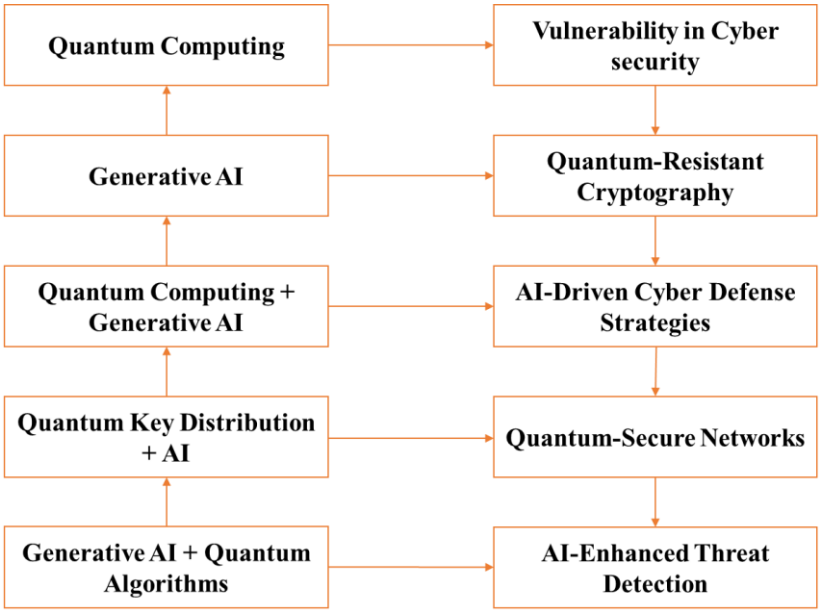

Figure 2. Interaction between Generative AI and Quantum Computing

Integration of the Generative AI and Quantum illustrated in Figure 2, the Quantum computing into cyber security begins with recognizing that quantum computing threatens existing encrypting encryption methods, such as RSA. Generative AI enhances this landscape by

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

designing new encryption algorithms and simulating potential cyber threats, leading to the development of quantum-resistant cryptography that is immune to quantum attacks. Additionally, generative AI aids in simulating cyber-attacks and formulating countermeasures, ensuring proactive defense strategies. The synergy between quantum computing's capability to process vast data and AI predictive power facilitates real-time threat identification and neutralization. Furthermore, combining QKD with AI strengthens communication channels for secure data transmission. Ultimately, the collaboration between generative AI and quantum computing improves anomaly detection, enhancing the accuracy of threat detection. This dynamic interplay underscores the potential of these technologies to future-proof cyber security systems against emerging quantum-based threats [59].

Generative AI a Quantum computing offers significant advantage over traditional AI techniques in cyber security due to their ability to process vast amount of data rapidly and enhance security measures. Generative AI can automate threats detection and response through real time analysis of network data, identifying anomalies that may indicate breaches more efficiently than conventional methods. This capability allows security teams to act swiftly, reducing the risk of damage from cyber-attacks. Furthermore, quantum computing enhances these processes by enabling the handling of complex dataset at unprecedented speeds, facilitating real time threats analysis and the development of quantum-resistant encryption algorithm that protect against future quantum decryption threats. Together, these technologies not only improve the exactness and speed of the threat detection but likewise enables the creation of adaptive security systems that evolves with emerging threats, making them a more robust solution for modern cyber security challenges compared to traditional AI techniques [60].

Combining Generative AI and Quantum for Advanced Threat Detection

Generative AI has emerged as a powerful tool in cyber security, particularly for its ability to analyze vast dataset and generate insights that can pre-emptively identifies threats. When integrated with quantum computing, the potential for advanced threats detection is significantly amplified. Quantum computing accelerates AI processes by leveraging phenomena such as superposition, entanglement, and quantum tunnelling, enabling the simultaneous processing of multiple possibilities. This acceleration allows for quicker model training and the simulation of potential cyber-attacks, which enhances the predictive capabilities of generative AI systems. For instance, quantum-enhanced generative models can simulate various attack vectors in high-dimensional spaces, improving the accuracy of threat predictions and enabling organizations to develop proactive defense strategies against emerging threats. Moreover, techniques such as quantum-inspired generative models can mimic quantum mechanics principles to enhance creativity and diversity in output generation, further enriching threat detection abilities [61].

Quantum ML for Cyber Defense

The integration of quantum computing with machine learning algorithms has given rise to new paradigm known as Quantum Machine Learning (QML). QML enhances traditional machine learning techniques by utilizing quantum algorithms for tasks such as clustering and pattern

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

recognition. Recent studies indicate that quantum-enhanced clustering methods can process complex datasets more effectively than classical algorithms, leading to improved detection of anomalous behaviour indicative of cyber threats [62]. Additionally, quantum machine learning models have shown promise in predicting cyber-attacks by analyzing patterns in historical data, thereby facilitating better decision-making in defense systems. Techniques like quantum enhanced decision trees and support vector machines are being explored to improve the speed and exactness of classification tasks relevant to cyber security [63].

Quantum-Enabled Generative Models for Intrusion Detection

Quantum computing also plays a pivotal role in enhancing generative models specifically designed for IDS. By leveraging quantum computings computational power, these models can analyze intricate attack vectors with greater precision and speed [64]. For example, quantum-enhanced adversarial AI techniques can identify potential exploits more rapidly than their classical counterparts, significantly reducing response times to threats. The incorporation of quantum algorithms into generative models allows for the generation of synthetic data that mimics real-world attack scenarios, providing organizations with robust training datasets that improve the performance of their IDS. Furthermore, techniques such as Quantum Generative Adversarial Networks (QGANs) are being developed to enhance the detection of complex attack patterns through adversarial training processes [65].

6. Comparative Analysis

Different methods are used to defense cyber security through Generative AI and Quantum. Table 1 depicts objective methods and result of the cyber-attacks and security by different prevailing studies.

Table 1. Comparative Analysis of Existing Studies

S.NO	Reference	Objective	Method	Result	Limitation
1	[13]	To explore the impact of generative AI on cyber security practices and defenses.	Current applications of generative AI in cyber security.	Identified key areas where generative AI enhances threat detection and response capabilities.	Limited focus on specific case studies or empirical data supporting claims.

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2	[14]	To assess the challenges and opportunities presented by generative AI in protecting critical infrastructure.	Qualitative analysis of generative AI applications in critical infrastructure security.	Highlighted the potential for generative AI to improve resilience against cyber threats in critical systems.	Challenges related to implementation and integration with existing systems were not deeply explored.
3	[15]	To investigate the role of generative AI in red teaming and its implications for quantum cryptography.	Case study approach examining red teaming techniques using generative AI and NLP.	Demonstrated how generative AI can enhance red teaming efforts by simulating advanced attack scenarios.	Focused primarily on theoretical implications rather than practical applications in real-world settings
4	[51]	To analyze how generative AI can be used in social engineering attacks like phishing.	Empirical analysis of phishing attacks utilizing generative AI techniques for deception.	Provided insights into the effectiveness of generative AI in crafting convincing phishing messages.	Limited scope on defensive measures against such attacks using generative AI technologies.
5	[52]	To compare different GAN architectures for generating malicious cyber-attack data for	Experimental comparison of various GAN architectures for data generation in cyber security contexts.	Identified optimal GAN architectures that produce realistic malicious data for training	The study may not fully account for the diversity of real-world attack scenarios

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

		training purposes.		security models.	encountered in practice
6	[55]	To investigate the potential applications of quantum technologies in enhancing cyber security.	Comprehensive analysis of quantum communication and cryptographic techniques.	Identified promising applications for quantum technologies in securing communications and data integrity.	Limited focus on practical implementation challenges in real-world scenarios.
7	[56]	To examine the intersection of AI and quantum cryptography in improving security protocols.	Theoretical exploration of AI applications in enhancing quantum cryptographic methods.	Proposed frameworks for integrating AI with quantum cryptography to bolster cyber security measures.	Theoretical nature may not address practical deployment issues effectively.
8	[57]	To develop a new encryption model using quantum key distribution for enhanced cloud security.	Design and implementation of a novel encryption model combining multi-qubits QKD with attribute-based encryption.	Demonstrated improved security features for cloud data protection against unauthorized access.	The complexity of implementation may limit adoption in existing cloud infrastructures.

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

9	[59]	To explore how the combination of quantum computing and AI can enhance cyber security solutions.	Analytical approach discussing potential synergies between AI algorithms and quantum computing capabilities.	Suggested that integrating these technologies can lead to more robust security frameworks against cyber threats.	Limited empirical evidence supporting the proposed synergies; relies heavily on theoretical analysis.
10	[61]	To investigate the use of natural language processing (NLP) with quantum computing for threat detection.	Experimental study integrating NLP techniques with quantum algorithms for analyzing cyber threats.	Found enhanced accuracy in threat detection through combined methodologies using NLP with quantum computing	Challenges related to computational resource requirements were not addressed comprehensively.
11	[62]	To develop a neural network model utilizing quantum principles for classifying DDoS attacks.	Model development using a hybrid approach combining neural networks with quantum computing techniques.	Achieved improved classification accuracy for DDoS attacks compared to classical models	The complexity of the model may hinder real-time application in operational environments.
12	[63]	To optimize machine learning algorithms using quantum computing for proactive cyber	Optimization techniques applied to enhance machine learning algorithms through quantum	Demonstrated significant improvements in processing speed and predictive accuracy for	Practical implementation challenges remain unaddressed; theoretical optimizations may not

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

		security measures.	computing capabilities.	cyber threat identification	translate directly to practice.
13	[64]	To explore the integration of federated learning with quantum computing for securing IoT devices in future networks.	Conceptual framework discussing federated learning approaches enhanced by quantum technologies.	Proposed a novel approach to enhance IoT security through decentralized learning mechanisms powered by quantum capabilities.	Limited exploration of real-world feasibility or case studies demonstrating effectiveness.

7. Challenges and Future Directions

Various challenges faced by the studies are

- The critical challenge of efficient resource allocation with quantum networks, particularly due to qubits variability and the inherent complexity of network management [65].
- The potential for generative AI to inadvertently expose sensitive information raises ethical and privacy issues, as noted by [43], which can complicate its deployment in real-world scenarios.
- The paper also highlight challenges related to scalability when deploying AI models across large networks or datasets, making it difficult to maintain performance as demands increase.
- The paper limited in emphasizing the necessity for large volumes of high quality data to train effective AI model [5, 7].

Future Direction

The future direction for enhancing cyber security through generative AI and quantum innovations emphasizes the development of adaptive security systems that can intelligently evolve in response to emerging threats. Research should prioritize the creation of quantum resistant encryption algorithms to defend data against potential quantum decryption methods, ensuring data integrity in a post quantum world. Moreover, leveraging quantum computing for real-time threat analysis will facilitate rapid responses to cyber-attacks, while association

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

between AI and quantum technologies can optimize encryption protocols for improved security. Enhancing the interpretability of AI systems is important, alongside efforts to reduce bias in training datasets to ensure fair and effective outcomes. Furthermore, advancing automation in incident response will enable AI models to proactively neutralize threats before they materialize. Establishing unified frameworks that integrate generative AI and quantum innovations will be critical for developing resilient security infrastructures capable of withstanding increasingly refined cyber threats. Technically includes realizing predictive threat intelligence through advanced machine learning algorithms, developing dynamic flexibility in security systems that utilize real time data feeds, enhancing automated incident response protocols, integrating behavioural analytics to detect insider threats, and establishing holistic adaptive security frameworks that encompass the pillars of predict, prevent, detect, and respond. By addressing these areas, the integration of generative AI and quantum computing has the potential to significantly transform the cyber security landscape, ensuring robust defenses against future challenges.

To further advance this capable joining of technologies, future research should not only focus on the development of quantum-resistant algorithms but also explore their implementation in diverse environments to assess performance under various operational conditions. Also, fostering interdisciplinary collaborations between cyber security experts and quantum physicists can lead to innovative solutions that leverage both fields' strengths. It is also vital to establish standardized protocols for integrating AI driven analytics with quantum computing capabilities to streamline deployment across organizations. Furthermore, enhancing educational initiatives aimed at developing a skilled workforce proficient in both AI and quantum technologies can help bridge the current talent gap in this domain. Continuous evaluation of ethical considerations surrounding AI applications in cyber security is crucial to mitigate risks associated with bias and ensure equitable access to advanced security measures across different sectors. Lastly, conducting longitudinal studies on the effectiveness of these technologies over time will provide valuable insights into their resilience against evolving cyber threats. By arranging these recommendations, researchers can pave the way for a more secure digital future that effectively harnesses the potential of cutting-edge technologies.

8. Critical Analysis

A Critical analysis is conducted concerning various factors leverages by generative AI and Quantum innovation in cyber defense. This analysis focuses on different methods employed, such as generative models and quantum algorithms, to enhance the accuracy of threats detection and response across all domains. Generative AI, particularly through techniques like generative AI and Quantum in cyber security.

Received: August 09,2025

International Journal of Applied Mathematics
Volume 38 No. 8s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

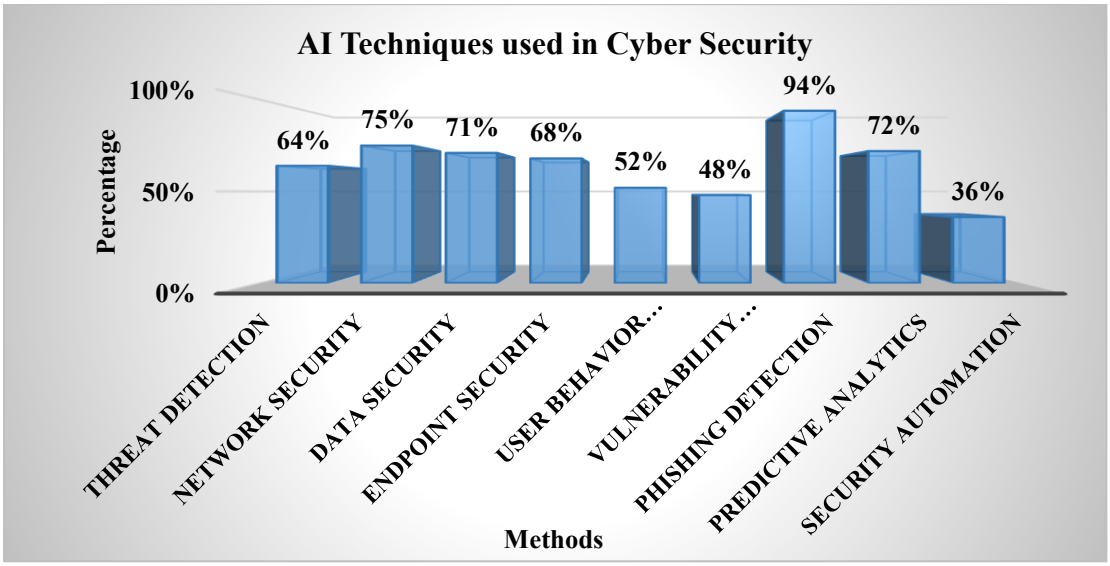

Figure 3. AI Techniques used in Cyber Security

The Figure 3, provides an overview of the different types of AI methods used in cyber security, showing how they are applied in different fields. Most notably, research focuses on threat detection and network security, with 64% and 75% of studies dedicated to these techniques, respectively. Data security 71% and endpoint security 68% also attract significant attention, highlighting their importance in protecting information and devices. User behaviour analytics 52% and vulnerability management 48% indicate a growing interest in understanding user actions and identifying system weaknesses. Phishing detection is particularly impressive, with a 94% accuracy rate in a specific study, showing the effectiveness of AI in combating this common threat. Predictive analytics 72% and security automation 36% also show ongoing efforts to improve proactive measures and streamline security processes. In general, the data shows a strong focus on using AI methods to enhance cyber security outcomes in critical areas.

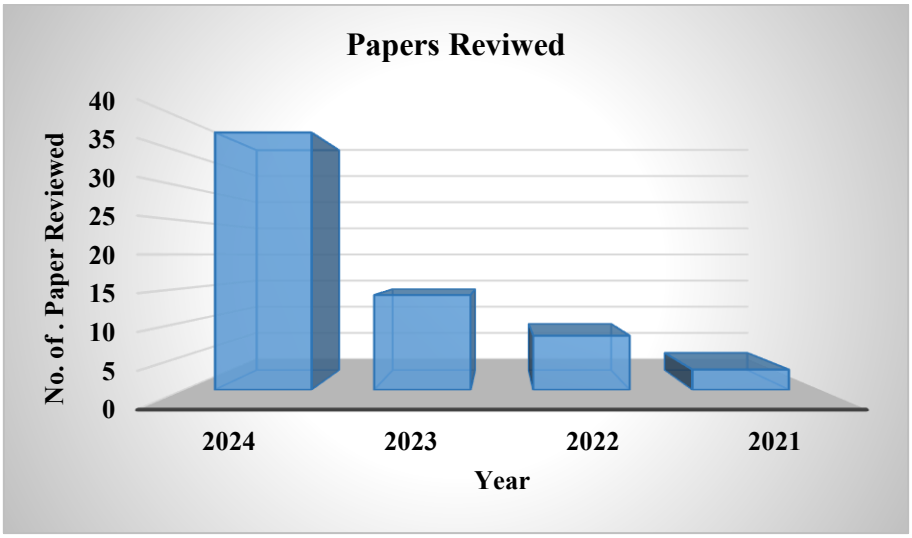

Figure 4. Number of papers Reviewed

Received: August 09,2025

International Journal of Applied Mathematics
Volume 38 No. 8s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The Figure 4, represent data presented in the quantity of papers reviewed in the realm of cyber security from 2021 to 2024. Initially, there were only 3 papers reviewed in 2021, but this number increased slightly to 8 in the following year, 2022. The upward trend persisted in 2023 with 14 papers reviewed, and by 2024, the number spiked to 38. This pattern highlights a growing interest and broadening of research in the cyber security domain, signalling the heightened significance of tackling evolving threats and creating novel solutions.

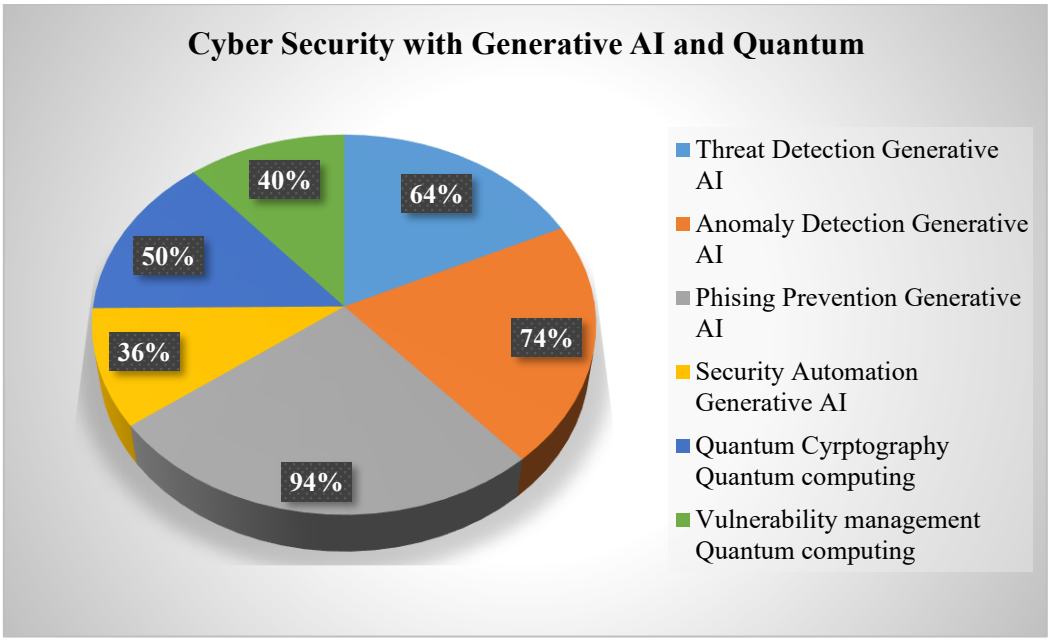

Figure 5. Cyber Security wit Generative AI and Quantum

The Figure 5, illustrates how generative AI and quantum computing are utilized in different cyber security areas, showing the percentage of studies that concentrate on each technique. In threat detection, generative AI is widely used, with 64% of studies focusing on this area, while anomaly detection sees even higher usage at 71%, demonstrating its effectiveness in identifying unusual activities. Phishing prevention has shown notable success, with one study reporting a detection accuracy of 94%. Generative AI also plays a role in security automation (36%) and predictive analytics 72%, indicating its contribution to enhancing proactive security measures. In contrast, quantum computing is anticipated to be utilized in quantum cryptography 50% and vulnerability management 40%, underscoring its potential in improving cyber security frameworks. Overall, the data suggests a strong interest in leveraging generative AI and quantum innovations to enhance security practices in various fields.

9. Conclusion

The combination of generative AI and quantum computing has the potential to transform cyber security strategies, providing new solutions to combat increasingly sophisticated cyber threats. While traditional defense methods are important, they are not enough to defend against the advanced tactics used by cyber criminals today. Generative AI has already shown promise in improving threat detection, automating responses to incidents, and identifying vulnerabilities by learning from past events. However, challenges such as interpreting AI models, biased data,

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and relying too heavily on automated systems must be addressed to ensure the reliability of AI driven solutions. The rapid progress of quantum computing poses a threat to conventional encryption methods, requiring the development of new quantum resistant algorithms. Despite obstacles, the merging of generative AI and quantum technology offers a proactive approach to creating resilient and adaptable cyber defense systems. By combining both technologies, organizations can establish dynamic and self-evolving security frameworks capable of predicting and countering emerging threats in real-time. Further research is needed to overcome technical barriers in integrating AI and quantum computing, especially in encryption, data integrity, and system transparency. This review emphasizes the importance of a comprehensive approach that utilizes the strengths of AI and quantum technologies to develop a new wave of cyber security solutions that are not just reactive but also proactive in protecting sensitive information and critical infrastructure. The future of cyber security depends on embracing these innovative technologies to ensure defense mechanisms evolve alongside the ever-changing cyber threat landscape.

Reference

[1] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *Cyber Security and Applications,* vol. 2, p. 100031, 2024.

[2] N. G. Camacho, "The Role of AI in Cybersecurity: Addressing Threats in the Digital Age," *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023,* vol. 3, no. 1, pp. 143-154, 2024.

[3] Y. Zheng, Z. Li, X. Xu, and Q. Zhao, "Dynamic defenses in cyber security: Techniques, methods and challenges," *Digital Communications and Networks,* vol. 8, no. 4, pp. 422-435, 2022.

[4] R. Menear, "Building a human firewall to keep your organisation secure," *Network Security,* vol. 2024, no. 5, 2024.

[5] M. A. Shyaa, N. F. Ibrahim, Z. Zainol, R. Abdullah, M. Anbar, and L. Alzubaidi, "Evolving cybersecurity frontiers: A comprehensive survey on concept drift and feature dynamics aware machine and deep learning in intrusion detection systems," *Engineering Applications of Artificial Intelligence,* vol. 137, p. 109143, 2024.

[6] M. I. Khan, A. Arif, and A. R. A. Khan, "The Most Recent Advances and Uses of AI in Cybersecurity," *BULLET: Jurnal Multidisiplin Ilmu,* vol. 3, no. 4, pp. 566-578, 2024.

[7] S. R. Mamidi, "Future Trends in AI Driven Cyber Security," *IRE Journal, August,* 2024.

[8] N. Kunle-Lawanson, "The role of AI in information security risk management," *World Journal of Advanced Engineering Technology and Sciences,* vol. 7, no. 2, pp. 308-319, 2022.

[9] M. Wang, "Generative AI: A New Challenge for Cybersecurity," *Journal of Computer Science and Technology Studies,* vol. 6, no. 2, pp. 13-18, 2024.

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[10] H. Sinha, "The identification of network intrusions with generative artificial intelligence approach for cybersecurity," *Journal of Web Applications and Cyber Security,* vol. 2, no. 2, pp. 20-29, 2024.

[11] I. H. Sarker, "Generative AI and Large Language Modeling in Cybersecurity," in *AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability*: Springer, 2024, pp. 79-99.

[12] A. Mehmood, A. Shafique, M. Alawida, and A. N. Khan, "Advances and vulnerabilities in modern cryptographic techniques: A comprehensive survey on cybersecurity in the domain of machine/deep learning and quantum techniques," *IEEE Access,* vol. 12, pp. 27530-27555, 2024.

[13] K. Curran, E. Curran, J. Killen, and C. Duffy, "The role of generative AI in cyber security," *Metaverse,* vol. 5, no. 2, 2024.

[14] Y. Yigit *et al.*, "Critical infrastructure protection: Generative ai, challenges, and opportunities," *arXiv preprint arXiv:2405.04874,* 2024.

[15] P. Radanliev, R. D. De, and S. Omar, "Red Teaming Generative AI/NLP, the BB84 quantum cryptography protocol and the NIST-approved Quantum-Resistant Cryptographic Algorithms," *Oxford University Research Archive,* 2023.

[16] M. Alauthman *et al.*, "Quantum Computing for Cybersecurity: A Comparative Study of Classical and Quantum Techniques," in *Innovations in Modern Cryptography*: IGI Global, 2024, pp. 75-99.

[17] A. C. Chen, "Post-Quantum Cryptography Neural Network," *arXiv preprint arXiv:2402.16002,* 2024.

[18] G. Alagic *et al.*, "Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process," ed: Gorjan Alagic, Maxime Bros, Pierre Ciadoux, David Cooper, Quynh Dang, Thinh …, 2024.

[19] M. T. Arefin, M. R. Uddin, N. A. Evan, and M. R. Alam, "Enterprise network: Security enhancement and policy management using next-generation firewall (NGFW)," in *Computer Networks, Big Data and IoT: Proceedings of ICCBI 2020*, 2021: Springer, pp. 753-769.

[20] P. Vanin *et al.*, "A study of network intrusion detection systems using artificial intelligence/machine learning," *Applied Sciences,* vol. 12, no. 22, p. 11752, 2022.

[21] Z. Azam, M. M. Islam, and M. N. Huda, "Comparative analysis of intrusion detection systems and machine learning based model analysis through decision tree," *IEEE Access,* 2023.

[22] K. Parveen, "Advanced techniques of malware evasion and bypass in the age of antivirus," *International Journal for Electronic Crime Investigation,* vol. 8, no. 3, 2024.

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[23] M. Amin, "The Importance of Cybersecurity and Protecting of Digital Assets and Understanding the Role of Cybersecurity Laws in Safeguarding Digital Assets," *Indian Journal of Public Administration,* vol. 70, no. 3, pp. 493-501, 2024.

[24] F. Nabi and X. Zhou, "Enhancing intrusion detection systems through dimensionality reduction: A comparative study of machine learning techniques for cyber security," *Cyber Security and Applications,* p. 100033, 2024.

[25] I. Naseer, "The role of artificial intelligence in detecting and preventing cyber and phishing attacks," *European Journal of Advances in Engineering and Technology,* vol. 11, no. 9, pp. 82-86, 2024.

[26] S. Han, M. Xie, H.-H. Chen, and Y. Ling, "Intrusion detection in cyber-physical systems: Techniques and challenges," *IEEE systems journal,* vol. 8, no. 4, pp. 1052-1062, 2014.

[27] A. F. Al Naim and A. M. Ghouri, "Exploring the Role of Cyber Security Measures (Encryption, Firewalls, and Authentication Protocols) in Preventing Cyber-Attacks on E-commerce Platforms," *International Journal of eBusiness and eGovernment Studies,* vol. 15, no. 1, pp. 44-469, 2023.

[28] P. Kaushal and P. Kaur, "Cyber Security Techniques Architecture and Design: Cyber-Attacks Detection and Prevention," in *Advancing Cyber Security Through Quantum Cryptography*: IGI Global, 2025, pp. 231-258.

[29] C. Park, J. Lee, Y. Kim, J.-G. Park, H. Kim, and D. Hong, "An enhanced AI-based network intrusion detection system using generative adversarial networks," *IEEE Internet of Things Journal,* vol. 10, no. 3, pp. 2330-2345, 2022.

[30] M. Roshanaei, M. R. Khan, and N. N. Sylvester, "Enhancing cybersecurity through AI and ML: Strategies, challenges, and future directions," *Journal of Information Security,* vol. 15, no. 3, pp. 320-339, 2024.

[31] G. Mumtaz *et al.*, "Classification and prediction of significant cyber incidents (SCI) using data mining and machine learning (DM-ML)," *IEEE Access,* vol. 11, pp. 94486-94496, 2023.

[32] M. Khan and L. Ghafoor, "Adversarial Machine Learning in the Context of Network Security: Challenges and Solutions," *Journal of Computational Intelligence and Robotics,* vol. 4, no. 1, pp. 51-63, 2024.

[33] G. Begum, S. Z. Ul Huq, and A. S. Kumar, "Fuzzy K-Means with M-KMP: a security framework in pyspark environment for intrusion detection," *Multimedia Tools and Applications,* pp. 1-23, 2024.

[34] M. Amouei, M. Rezvani, and M. Fateh, "RAT: Reinforcement-learning-driven and adaptive testing for vulnerability discovery in web application firewalls," *IEEE Transactions on Dependable and Secure Computing,* vol. 19, no. 5, pp. 3371-3386, 2021.

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[35] H. J. Hadi, Y. Cao, S. Li, Y. Hu, J. Wang, and S. Wang, "Real-time collaborative intrusion detection system in uav networks using deep learning," *IEEE Internet of Things Journal,* 2024.

[36] A. K. Samha, N. Malik, D. Sharma, and P. Dutta, "Intrusion detection system using hybrid convolutional neural network," *Mobile Networks and Applications,* pp. 1-13, 2023.

[37] N. Ganesh, R. Shankar, M. Mahdal, J. S. Murugan, J. S. Chohan, and K. Kalita, "Exploring Deep Learning Methods for Computer Vision Applications across Multiple Sectors: Challenges and Future Trends," *CMES-Computer Modeling in Engineering & Sciences,* vol. 139, no. 1, pp. 103-141, 2024.

[38] M. S. Akhtar and T. Feng, "Detection of malware by deep learning as CNN-LSTM machine learning techniques in real time," *Symmetry,* vol. 14, no. 11, p. 2308, 2022.

[39] S. I. Ansarullah, A. W. Wali, I. Rasheed, and P. Z. Rayees, "AI-powered strategies for advanced malware detection and prevention," in *The Art of Cyber Defense*: CRC Press, 2024, pp. 3-24.

[40] A. Al Tawil, L. Almazaydeh, D. Qawasmeh, B. Qawasmeh, M. Alshinwan, and K. Elleithy, "Comparative Analysis of Machine Learning Algorithms for Email Phishing Detection Using TF-IDF, Word2Vec, and BERT," *Comput. Mater. Contin,* vol. 81, p. 3395, 2024.

[41] N. Altwaijry, I. Al-Turaiki, R. Alotaibi, and F. Alakeel, "Advancing Phishing Email Detection: A Comparative Study of Deep Learning Models," *Sensors,* vol. 24, no. 7, p. 2077, 2024.

[42] O. Krishnamurthy, "Impact of Generative AI in Cybersecurity and Privacy," *International Journal of Advances in Engineering Research,* vol. 27, pp. 26-38, 2024.

[43] K. Palani, J. Kethar, S. Prasad, and V. Torremocha, "Impact of AI and Generative AI in transforming Cybersecurity," *Journal of Student Research,* vol. 13, no. 2, 2024.

[44] G. Al-Kateb, I. Khaleel, and M. Aljanabi, "CryptoGenSec: A Hybrid Generative AI Algorithm for Dynamic Cryptographic Cyber Defence," *Mesopotamian Journal of CyberSecurity,* vol. 4, no. 3, pp. 22-35, 2024.

[45] M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, "From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy," *IEEE Access,* 2023.

[46] A. Valavanidis, "Artificial Intelligence (AI) Applications," *Department of Chemistry, National and Kapodistrian University of Athens, University Campus Zografou,* vol. 15784, 2023.

[47] P. Radanliev and O. Santos, "Adversarial Attacks Can Deceive AI Systems, Leading to Misclassification or Incorrect Decisions," 2023.

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[48] N. Zhang, M. Ebrahimi, W. Li, and H. Chen, "Counteracting dark Web text-based CAPTCHA with generative adversarial learning for proactive cyber threat intelligence," *ACM Transactions on Management Information Systems (TMIS),* vol. 13, no. 2, pp. 1-21, 2022.

[49] M. Adiban, S. M. Siniscalchi, and G. Salvi, "A step-by-step training method for multi generator GANs with application to anomaly detection and cybersecurity," *Neurocomputing,* vol. 537, pp. 296-308, 2023.

[50] N. Khan, K. Ahmad, A. A. Tamimi, M. M. Alani, A. Bermak, and I. Khalil, "Explainable AI-based Intrusion Detection System for Industry 5.0: An Overview of the Literature, associated Challenges, the existing Solutions, and Potential Research Directions," *arXiv preprint arXiv:2408.03335,* 2024.

[51] M. Schmitt and I. Flechais, "Digital Deception: Generative artificial intelligence in social engineering and phishing," *Artificial Intelligence Review,* vol. 57, no. 12, pp. 1-23, 2024.

[52] N. Peppes, T. Alexakis, K. Demestichas, and E. Adamopoulou, "A comparison study of generative adversarial network architectures for malicious cyber-attack data generation," *Applied Sciences,* vol. 13, no. 12, p. 7106, 2023.

[53] S. De, M. Bermudez-Edo, H. Xu, and Z. Cai, "Deep generative models in the industrial internet of things: a survey," *IEEE Transactions on Industrial Informatics,* vol. 18, no. 9, pp. 5728-5737, 2022.

[54] F. Raheman, "The future of cybersecurity in the age of quantum computers," *Future Internet,* vol. 14, no. 11, p. 335, 2022.

[55] V. Vasani, K. Prateek, R. Amin, S. Maity, and A. D. Dwivedi, "Embracing the quantum frontier: Investigating quantum communication, cryptography, applications and future directions," *Journal of Industrial Information Integration,* p. 100594, 2024.

[56] P. Radanliev, "Artificial intelligence and quantum cryptography," *Journal of Analytical Science and Technology,* vol. 15, no. 1, p. 4, 2024.

[57] K. K. Singamaneni, G. Muhammad, and Z. Ali, "A novel multi-qubit quantum key distribution Ciphertext-policy attribute-based encryption model to improve cloud security for consumers," *IEEE Transactions on Consumer Electronics,* 2023.

[58] U. Mmaduekwe and E. Mmaduekwe, "Cybersecurity and Cryptography: The New Era of Quantum Computing," *Current Journal of Applied Science and Technology,* vol. 43, no. 5, pp. 41-51, 2024.

[59] A. Ahmadi, "Quantum Computing and Artificial Intelligence: The Synergy of Two Revolutionary Technologies," *Asian Journal of Electrical Sciences,* vol. 12, no. 2, pp. 15-27, 2023.

[60] A. K. Bishwas and M. Sen, "Strategic Roadmap for Quantum-Resistant Security: A Framework for Preparing Industries for the Quantum Threat," *arXiv preprint arXiv:2411.09995,* 2024.

Received: August 09,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[61] P. Ramya, R. Anitha, J. Rajalakshmi, and R. Dineshkumar, "Integrating Quantum Computing and NLP for Advanced Cyber Threat Detection," *Journal of Cybersecurity & Information Management,* vol. 14, no. 2, 2024.

[62] M. Y. Küçükkara, F. Atban, and C. Bayılmış, "Quantum-Neural Network Model for Platform Independent Ddos Attack Classification in Cyber Security," *Advanced Quantum Technologies,* vol. 7, no. 10, p. 2400084, 2024.

[63] C. Rosa-Remedios and P. Caballero-Gil, "Optimizing quantum machine learning for proactive cybersecurity," *Optimization and Engineering,* pp. 1-33, 2024.

[64] D. Javeed, M. S. Saeed, I. Ahmad, M. Adil, P. Kumar, and A. N. Islam, "Quantum-empowered federated learning and 6G wireless networks for IoT security: Concept, challenges and future directions," *Future Generation Computer Systems,* 2024.

[65] M. Xu *et al.*, "Generative AI-enabled Quantum Computing Networks and Intelligent Resource Allocation," *arXiv preprint arXiv:2401.07120,* 2024.

Received: August 09,2025