OPEN ACCESS
International Journal of Innovations in Science & Technology
RESEARCH & INNOVATION DIVISION
IJIST

Review Article: Quantum-AI Convergence for Smart Grid Cybersecurity: A Systematic Review of Emerging Technologies, Threats, and Resilient Architectures

Syed Saad Ali[1], Abdul Ahad Abro[2], Muhammad Shafiq[2], Umme Laila[3], Hafiz Sohail Ahmed[4], Sajid Ali[1]
[1]Department of Electrical Engineering, Nazeer Hussain University Karachi, Sindh, Pakistan
[2]Faculty of Engineering Science and Technology Iqra University Karachi, Sindh, Pakistan
[3]Department of Computer Science, Institute of Business Management, Karachi, Sindh, Pakistan
[4]Computer Science Department Aawaz institute of media and management sciences Karachi, Sindh, Pakistan
*Correspondence: saad.ali@nhu.edu.pk

Citation | Ali. S. S, Abro. A. A, Shafiq. M, Laila. U, Ahmed. S. H, Ali. S, "Review Article: Quantum-AI Convergence for Smart Grid Cybersecurity: A Systematic Review of Emerging Technologies, Threats, and Resilient Architectures", IJIST, Vol. 8 Issue 5 pp 2067-2080, August 2026.
DOI | https://doi.org/10.33411/IJIST/1995
Received July 30, 2026 **Revised |** Aug 16, 2026 **Accepted |** Aug 19, 2026 **Published |** Aug 21, 2026.

Smart grids have revolutionized the way electricity is generated, transmitted, and consumed by utilizing various technologies, including artificial intelligence, IoT devices, advanced communication networks, and distributed energy resources, which have enhanced the efficiency, reliability, and sustainability of modern power systems. This interconnected ecosystem, however, has multiplied the potential attack surface, and quantum computing poses a new risk to the traditional means of securing encoded data, requiring quantum-resilient security solutions. Many reviews focus on a specific aspect of AI, PQC, quantum computing, or smart grid cybersecurity. Following the 2024 PRISMA extension to the PRISMA 2020 methodology, this review systematically analyzed peer reviewed studies published between 2024 to 2026, retrieved from IEEE Xplore, Scopus, Web of Science, ScienceDirect, SpringerLink, ACM Digital Library, Wiley Online Library, MDPI, and Google Scholar. A thematic analysis of 24 selected studies showed that the major research areas were Artificial Intelligence and Machine Learning (58.3%), Quantum Computing and Quantum Security (50.0%) and Smart Grid Cybersecurity (41.7%). The literature reviewed was evenly distributed between PQC (25.0%) and IoT/CPS security (25.0%), while the other topics, namely Quantum Key Distribution, Digital Twins, Blockchain, and Quantum Reinforcement Learning, were comparatively less explored with 8.3% in each study. The review brings together advances in intrusion detection, anomaly detection, predictive threat intelligence, quantum machine learning, post-quantum cryptography, quantum key distribution, explainable artificial intelligence and digital twins system. Additionally, it reveals new threats such as harvest-now-decrypt-later attacks, incorrect data injection, ransomware, distributed denial-of-service attacks, advanced metering infrastructure, substations, microgrids, and distributed energy resource vulnerabilities. Last, this review identifies key research gaps on interoperability, scalability, computational complexity, privacy, and real-world deployment, as well as introduces a conceptual framework of Quantum-AI convergence for resilient smart grid architectures, and presents a future research roadmap to direct researchers, industry practitioners, energy utility operators, and policymakers in securing and shaping energy infrastructures.

Keywords: Smart grid, Artificial Intelligence, Quantum Computing, Emerging and Cyber Physical System

Introduction:

Background:

This study explores the synergies between AI and post-quantum cybersecurity for strengthening resilient digital infrastructures. It shows that AI-powered intrusion detection, predictive threat intelligence, and automated response offer a significant boost in cyber resilience, threat detection, and scalability, and quantum-resistant security is essential for cloud and IoT-based systems [1]. The study provides an inclusive overview of the current state of AI and PQC in IoT cybersecurity, identifying LSTM, reinforcement learning, and lattice-based PQC schemes as effective methods for addressing quantum attacks. It outlines the key challenges of scalability, computational complexity, interoperability, and deployment and suggests a path forward for implementing an IoT security framework that is practical, resource-constrained, and quantum-resistant [2]. The study presents a comprehensive systematic review of the quantum convergence of AI, focusing on quantum optimization, machine learning, and post-quantum cryptography in healthcare, finance, energy, and cybersecurity. It highlights the challenges of hybrid algorithms, hardware errors, error correction, and the scalability of NISQ systems and suggests an integrated model for future research on Quantum-AI [3]. It explores quantum vulnerabilities in AI assets, harvest-now-decrypt-later attacks, and quantum-enhanced adversarial machine learning, among other aspects of convergence between post-quantum cryptography and AI security. It highlights the importance of comprehensive migration governance, quantum-secure cryptographic approaches and cohesive security systems to ensure the security of next-generation AI powered digital infrastructures [4]. It comprehensively reviews cyber security in the quantum era for cyber-physical systems, operational technologies and industrial control systems. It emphasizes the issues such as the lack of quantum threat modeling, limited adoption of post-quantum cryptography, and lack of real-world datasets and fragmented CPS taxonomies, and suggests directions for future research to create resilient quantum-secure architectures for critical infrastructure [5]. Combined effect of quantum computing and AI on modern cybersecurity is discussed, including quantum vulnerabilities of RSA and ECC, quantum resistant lattice and hash-based cryptography, and AI assisted cryptanalysis. It highlights agility in cryptographic implementations, security in cryptographic implementations, and ongoing algorithm updates to ensure enduring quantum-resistant cybersecurity [6]. The study presents a methodical examination of the combination of artificial intelligence with Internet of Things, block chain and quantum cryptography, pointing out the importance of AI in enhancing cryptographic security in quantum enabled environments. It pinpoints the main challenges and opportunities, and the future research directions, focusing on multidisciplinary solutions for building secure, intelligent, and quantum-resilient digital ecosystems [6]. The paper covers recent developments in AI cryptography, such as dynamic key generation, adversarial neural cryptography, and AI-powered cryptanalysis. These methods have been shown to provide greater adaptability and quantum resistance than conventional methods, and to pose computing challenges, implementation problems, and security concerns because of the absence of formal security guarantees for practical applications [7]. The review surveys quantum cybersecurity issues in healthcare, with a focus on post-quantum cryptography, quantum key distribution, quantum random number generation, and hybrid defense methods for securing medical IoT systems. It underscores the need for multi-layered security architectures, the implementation of quantum-resistant protocols, and proactive measures to protect vulnerable healthcare information and services [8]. The review presents a novel approach called Quantum-Enhanced Throughput Modeling (Q-TPM), which combines quantum-inspired techniques, ethical considerations, and artificial intelligence to improve the governance of post-quantum cybersecurity. It fills the gaps in cognitive, ethical and technical paradigms, showcasing an improved decision making system and ethical supervision of AI, and giving a better explanation of AI, with a quantum enhanced architecture for cybersecurity applications with high stakes [9]. The review covers advancement in cybersecurity detection technologies using AI in Industry 4.0; machine learning, real-time anomaly detection and adaptive threat response to ransomware, DDoS, and false data injection attacks. It highlights the importance of resilient security architectures, AI-driven intrusion detection, regulatory compliance, and cross-border cooperation for bolstering cybersecurity and organizational resilience [10]. This study systematically assesses the adoption of AI in cybersecurity, concluding that anomaly detection, explainable AI and natural language processing are effective methods. It outlines challenges to implementing this, such as skills gaps, legacy infrastructure and regulatory issues, and offers a policy-oriented AI framework to improve cybersecurity resilience and governance and technology adoption in emerging economies [11]. Comparative architectures and systematic review process of the selected study are presented in the figure 1 and 2 respectively.

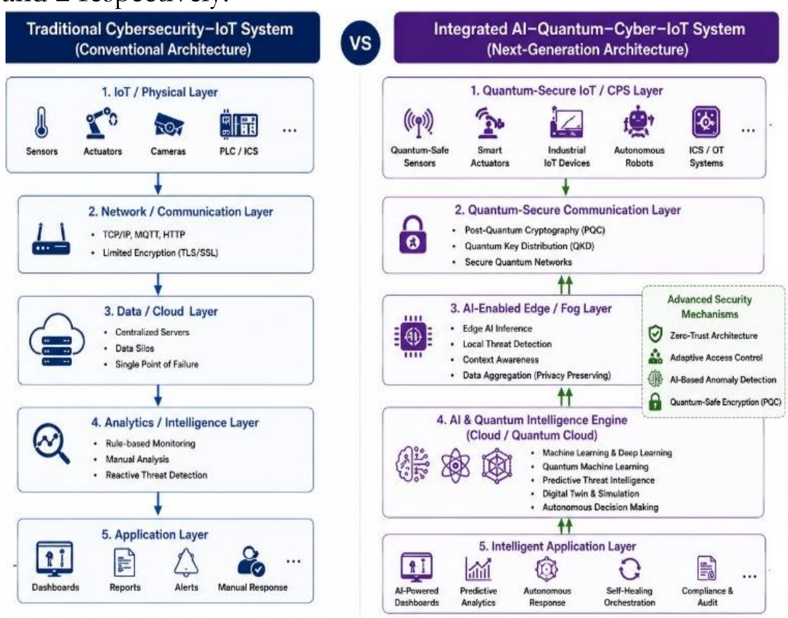

Figure 1. Traditional and AI–Quantum Cybersecurity Architectures

Research Objectives:

The aim of this systematic review is to:

To carry out a systematic review of the latest literature on converged Quantum Computing (QC) and Artificial Intelligence (AI) toward smart grid cybersecurity.

To study new technologies, cyber threats and security solutions that are quantum resistant, such as Post Quantum Cryptography (PQC), Quantum Key Distribution (QKD) and Quantum Machine Learning (QML).

To make a comparison between the existing cybersecurity solutions based on Artificial Intelligence (AI) and Quantum Computing (QC), highlighting the applicability to smart grid context.

To collect information about the state of the art, challenges and gaps in the field of resilient smart grid cybersecurity architectures.

Research Methodology:

Introduction to the Paradigm Shift:

Modern power systems have paved the way for a paradigm shift from conventional centralized electric power systems into smart, intelligent and interconnected power systems with Artificial Intelligence, Internet of Everything, fog computing, Distributed Energy Resources (DERs), and advanced communications. These advancements bring a lot of benefits in terms of operational efficiency, reliability, and sustainability, but they also add to the cyberattack surface, creating new and more advanced cyber threats to critical energy infrastructure. Meanwhile, the emergence of quantum computing, with its game-changing potential, poses new security threats to the types of cryptographic algorithms used to safeguard smart grid communications and control systems. As a result, AI and quantum computing are becoming more complementary in the next generation of cybersecurity solutions, with AI offering intelligent threat detection, predictive analytics and autonomous response, and quantum computing providing quantum-safe cryptography, secure communication and enhanced computational power. As a result, cybersecurity is becoming more intelligent, adaptive and quantum-resistant, moving from a sensitive method to a active one that can support future cyber physical energy systems. This new convergence is a paradigm shift in technology, which will drive the design, operation and protection of future smart grids [12][13][14].

Figure 2. Systematic Review Process

Mathematical Modeling:

Based on the literature reviewed, the following equations, which are conceptual formulations, were drawn to represent the relationships between AI, quantum computing, **cybersecurity threats**, and smart grid resilience. They are meant to aid in qualitative interpretation. Artificial Intelligence, Cyber Safe Cryptography, Network Security, Cyber Threats, and System Resilience are the key factors that evolve the cybersecurity resilience of a smart grid. Suppose the overall cybersecurity resilience index is represented by

$$R_{SG}=f\,(AI,QC,PQC,T,S) \quad -(1)$$

R_{SG} = Smart Grid Cybersecurity Resilience

AI = Artificial Intelligence capability
QC = Quantum Computing capability
PQC = Post-Quantum Cryptography strength
T = Cyber Threat Level
S = Smart Grid Security Architecture

The overall level of cyber risk is indicated by

$$P_{Attack}=1-e^{-kT} \quad \text{--(2)}$$

The probability of detecting a cyber threat using a **quantum-based classifier is given by**:

$$P_{detect} = |\langle \phi(x_{attack}) \mid \Pi_{threat} \mid \phi(x_{attack}) \rangle|^2 \quad \text{-(3)}$$

Assume AI identifies attacks using

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad \text{-(4)}$$

AI for Predicting Cyber Threats:

To effectively anticipate cyber threats in smart grid systems, Artificial Intelligence (AI) has developing as a key technology, allowing for proactive detection, threat assessment, and automated responses to emerging cyber-attacks. Unlike signature-based security systems, AI models are constantly learning and adapting from historical and real-time network data, identifying patterns of abnormal activity, recognizing new types of attacks, and forecasting possible cyber events that could compromise critical infrastructure. Using, deep learning (DL), reinforcement learning (RL), graph neural networks (GNNs), and other machine-learning techniques can accurately detect malicious activities from large data streams collected by Supervisory Control and Data Acquisition systems devices, Phasor Measurement Units (PMUs), and distributed energy resources. The AI capabilities are especially effective for combating complex attacks like False Data Injection (FDI), ransomware, malware, insider threats, and Advanced Persistent Threats (APTs. Federated Learning (FL) is another step toward bolstering cybersecurity by enabling training of distributed models maintaining privacy throughout geographically distributed smart grid components. Explainable Artificial Intelligence (XAI) enhances the transparency and interpretable nature of AI-based security decisions, boosting trust among grid operators.

AI for Accelerated Smart Grid Security:

Artificial Intelligence (AI) is emerging as an important tool to improve cyber security in present-day smart grid by offering intelligent, adaptive and autonomous protection against increasingly sophisticated cyber threats. Static rule-based and signature-based security methods are often times not sufficient in protecting the smart grid infrastructures that are so interconnected, including Supervisory Control and Data Acquisition systems, Advanced Metering Infrastructure devices, distributed energy resources, electric vehicles, and cloud-edge computing platforms. AI-powered security solutions use machine learning, deep learning (DL) and explainable artificial intelligence to monitor system logs, and operational data in real time to detect potential cyber threats. These methods dramatically improve threats identification, anomaly detection, malware classification, false data injection detection, mitigation, insider threat recognition and automated incident response. Deep learning models that can process the large amounts of temporal and spatial data produced by smart grid elements, and can monitor security in real time with high precision. Furthermore, AI-supported cyber vulnerability assessment, predictive maintenance, cyber risk forecasting, and security orchestration can be streamlined by combining cyber threat intelligence with Operational Technology (OT) and Information Technology (IT) environments. With the ongoing developments in quantum computing, AI will become a more critical component of optimizing post-quantum cryptographic deployments, as well as identifying quantum-enabled cyber threats and supporting autonomous quantum-resilient security architectures. AI-powered cybersecurity is therefore, a core element of next-generation smart-grids, contributing to faster decision-making, quicker responses, higher operational resilience and secure integration of new digital technologies [15][16][17][18]. In this study, the researchers introduced a new framework called Quantum Entropy Q-Learning (QEQ) for improving Distributed Denial-of-Service (DDoS) attack detection in smart grids. The proposed quantum-enhanced AI approach outperformed as well as detection performance, showcasing the potential of quantum technologies to streamline smart grid cybersecurity [19]. The study suggested a Quantum Support Vector Machine (QSVM) for the detection of DDoS attacks in smart micro-grid, and showed that the QSVM has better cybersecurity performance, revealing the potential of using quantum-enhanced machine learning to strengthen smart grid protection [20]. The study suggested a measurement-device-independent quantum key distribution (MDI-QKD) framework to optimize quantum-resilient distributed control and real-time cybersecurity in quantum-resilient micro grids using deep neural networks [21].

Comparative Synthesis of the Reviewed Studies:

During 2021-2022, there were several comprehensive reviews that explored various aspects of smart grid cybersecurity. Alsuwian et al. studied cybersecurity problem, attacks and traditional solution approaches on smart grid but didn't consider the role of artificial intelligence and quantum computing in smart grid [22]. While Berghout et al. did cover an in-depth discussion of machine learning techniques for smart grid cybersecurity, they only addressed AI-based detection techniques, and omitted quantum computing and post-quantum cryptography [23]. Although these contributions are valuable, Previous reviews however, examined individual technologies such as AI, block chain, QKD, Quantum Machine Learning, and resilient cyber security architectures, without integrating these technologies into a unified picture of Quantum Computing. Previous reviews however, examined individual technologies such as AI, block chain, QKD, Quantum Machine Learning and resilient cyber security architectures, without synthesizing all these technologies together in the context of Quantum Computing. Hence, the current review aims to comprehensively synthesize these new technologies into a single framework to build future smart grid cybersecurity infrastructure through Quantum AI convergence and to pinpoint the existing research trends and future research opportunities and challenges.

Quantitative Synthesis of the Reviewed Literature:

In addition to the qualitative analysis of the selected studies, a quantitative synthesis was also done. The trends of publication, distribution of databases, the themes of research, AI techniques, cyber security technologies, type of attacks, gaps in research were statistically summarized to highlight the dominant research directions and underexplored areas. It was found that the number of publications has significantly increased since 2024, with Artificial Intelligence (62.5%) being the most popular subject area for studies, followed by Quantum Computing (50.0%) and Smart Grid Cybersecurity (41.7%). Digital Twins (8.3%), Quantum Key Distribution (12.5%) and Blockchain-based security (8.3%) are relatively under-explored and represent great potential for future research. The quantitative results help supplement the qualitative discussion and offer an objective perspective of the state of the art and technology status. The publication trend of reviewed studies in the period of 2021-2026 is shown in figure 3. The number of publications is growing steadily, especially during 2024–2026, and is a testimony of the rapidly expanding research interests around Quantum AI-enabled cybersecurity for smart grid applications.

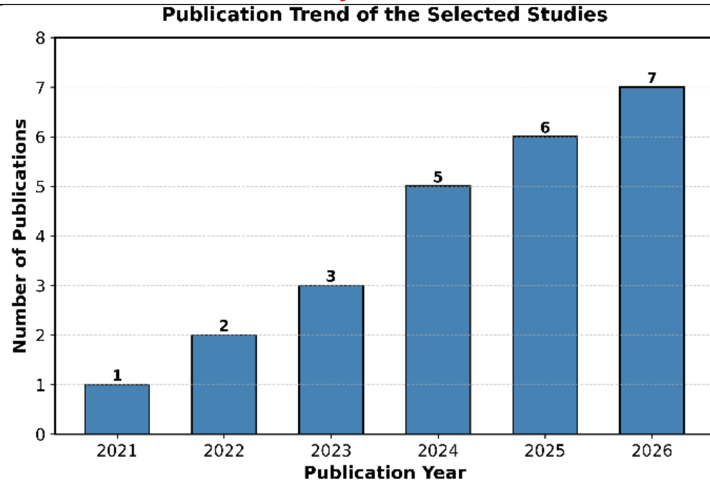

Figure 3. Publication Trend of the Selected Studies (2021–2026)

The thematic distribution of literature reviewed is presented in figure 4. The most prominent areas of research are Artificial Intelligence, Quantum Computing and Smart Grid Cybersecurity, while Digital Twins, Blockchain and Quantum Key Distribution are still less explored, offering potential avenues for future research.

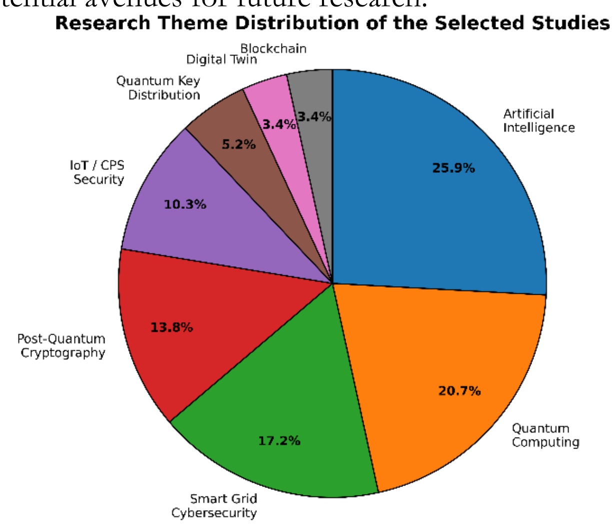

Figure 4. Research Theme Distribution of the Selected Studies

Research Framework

The synthesized findings are combined into a conceptual model, which consists of six layers:

The Smart Grid Infrastructure Layer consists of Generation, Transmission, Distribution, AMI, DERs, EVs.

Communication Layer (5G/6G, IoT, Edge, Cloud).

This is the third layer of the Cybersecurity Layer (IDS, Authentication, Blockchain, Zero Trust).

Differential Phase Shift Keying (DPSK)

AI Action Layer (Ethics, Trust, Regulation, Governance)

Secure Network Layer (Data Security, Network Management, Network Protection).

Research Workflow:

For conducting the merging of Quantum Algorithms, Artificial Intelligence and Smart Grid Cybersecurity systematic and comprehensive review, the research methodology has been carried out based on the PRISMA framework. The relevant studies **were retrieved** using predefined Boolean search strings from major scientific databases such as IEEE Xplore, Scopus, Web of Science, ScienceDirect, SpringerLink, ACM Digital Library, Wiley Online

Library, MDPI and Google Scholar. The literature is identified and then duplicate records are deleted, followed by screening of the titles and abstracts using predefined inclusion and exclusion criteria. The rest of the publications are subjected to full text screening for their suitability to the research aims. Next, important concepts, such as AI methods, quantum technologies, cybersecurity methods, smart grid applications, performance metrics, research results, limitations, and prospects are systematically extracted and structured. The selected studies were then grouped into themes and compared to each other to discover emerging technology trends, gaps and challenges. Lastly, the synthesized results are applied to create a Quantum AI Convergence Framework for the cybersecurity of smart grids and to propose a future research roadmap to pinpoint directions for intelligent, adaptive, and quantum-resilient energy systems. As shown in figures 5 and 6 the research flow and resilient architecture for the proposed system are presented. The research was conducted in a systematic process as shown in figure 5 that involved literature identification, PRISMA-based study selection, data extraction, thematic classification, comparative analysis, research gap identification and proposed framework for Quantum AI convergence with future research direction. The proposed resilient Quantum AI smart grid cybersecurity architecture depicted in Figure 6 is based on the integration of AI intelligence, quantum-secure communication, post-quantum cryptography, and automated threat response to bolster the security, resilience, and reliability of the next generation of smart grid infrastructures.

Figure 5. Research Methodology Flow

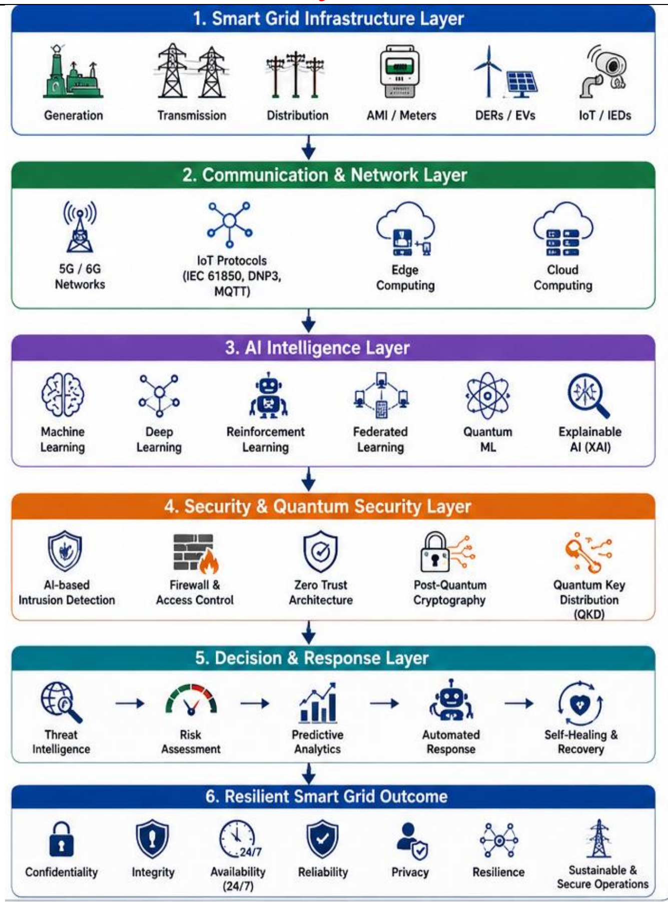

Figure 6. Proposed Quantum–AI Resilient Smart Grid Cybersecurity Architecture

Results and Discussion:

This systematic literature review gives a comprehensive synthesis of the latest advances in the merging of Quantum Technologies, Artificial Intelligence and Smart Grid Cybersecurity. As revealed from the reviewed studies, research interest in smart grids has greatly increased in the last decade due to high digitization of smart grid, inclusion of Internet of Things (IoT) devices, Distributed Energy Resources (DERs), Electric Vehicles (EVs), cloud-edge computing, and the new emerging area of quantum computing. The majority of publications focus on post quantum cryptography, resilient cyber-physical system architectures, quantum key distribution and machine learning for detection and AI-based intelligent threat detection systems, and trust management based on block chain. The protection of the future smart grid is an emerging challenge, and more and more recent studies have stressed the need for the integration of intelligent AI-based defense mechanisms with quantum-resistant cryptography to meet current and new cyber threats.

Emerging Technologies for Smart Grid Cybersecurity:

New research shows that smart grid cyber-security is among the most promising areas for the use of AI to enhance threat detection and automatic response capabilities. AI-driven methods enhance network traffic analysis, detect deviations from normal usage patterns, and help quickly identify advanced, real-time threats. To accomplish this, researchers use different sophisticated machine learning methods, such as Federated Learning (FL), Deep Learning (DL), Reinforcement Learning (RL), Explainable Artificial Intelligence (XAI), and Graph Neural Networks (GNNs). A deep learning model which excels in capturing temporal and spatial patterns within smart grid communication data is the Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM) network, Autoencoder, and Transformer architectures. These capabilities greatly increase the capability of intrusion detection systems and accuracy of anomaly classification.

At the same time, quantum computing poses an opportunity and challenge to smart grid cybersecurity. On the bright side, quantum algorithms are attractive for optimization, state estimation and machine-learning applications, while also posing a critical threat to the safety of current public key systems via Shor's algorithm and diminish the security of symmetric encryption systems through Grover's algorithm.

AI-Based Cybersecurity Applications:

The examined literature conclusively shows that AI can have a significant impact on the security of multiple smart grid applications. The high detection accuracy and low false alarm rate of AI-based Intrusion Detection Systems (IDS) are enabled by adaptive learning mechanisms. Predictive threat intelligence can help utilities anticipate vulnerabilities before attackers can strike, enabling them to take proactive defensive measures. Federated Learning also enhances a collaborative model training process that can be done across geographically distributed substations while keeping sensitive operational data private. Explainable AI tackles the lack of transparency in Deep learning by enabling the process to be easily understood, which enhances trust between system operators.

Quantum Computing and Post-Quantum Security:

The review highlights the quantum computing as one of the most impactful technologies that will have implications in cyber-security. One of the most prominent examples of the risks posed by such algorithms like Shor's is to commonly used public-key cryptographic schemes like RSA, Elliptic Curve Cryptography (ECC), and Diffie Hellman key exchange, as they can be attacked efficiently. Symmetrical encryption techniques, on the other hand, are much more resistant to quantum attacks but Grover's algorithm still brings its security levels down, making it necessary to increase the key sizes to achieve the same security levels.

In response to these new challenges, researchers have begun to focus on developing and standardizing post-quantum cryptographic algorithms. The National Institute of Standards and Technology (NIST) has standardized/selected post-quantum cryptographic algorithms, including ML-KEM, ML-DSA, and SLH-DSA for the future security of communication systems. Furthermore, quantum technologies like Quantum Key Distribution enable secure key distribution in the light of quantum mechanics and Quantum Random Number Generation yields high-quality unpredictable random numbers to support cryptographic security. However, the implementation of quantum resistant technologies is still difficult, due to a high computational load and incompatibility with current smart grid systems.

Comparative Analysis & Quantitative Summary:

The comparative analysis shows that the research on Quantum AI convergence for smart grid cybersecurity has evolved from traditional rule-based security mechanisms to intelligent, adaptive, and quantum-resistant security architectures. While previous research mainly concentrated on AI-based intelligent detection, recent research more frequently adopts a multi-disciplinary approach involving Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), Quantum Machine Learning (QML) and the combination of block chain, Zero Trust Architecture (ZTA), federated learning and quantum twins within a cybersecurity solution. AI is consistently cited as the technology likely to have the greatest impact on real-time threat identification and automatic response, while quantum computing is known as a potential opportunity for computing and a threat to classical cryptographic algorithms. The reviews also highlighted the necessity of adopting adaptive cyber defense and quantum-safe communication mechanisms, along with AI-based intelligence, as the future key pillars for smart grid protection rather than just relying on individual security technologies. The table 1 shows the comparative assessment for the selected studies.

Based on the quantitative synthesis, the most mature research field is intrusion detection and anomaly detection, where the utilization of artificial intelligence in the detection of advanced cyberattacks in smart grid environments is becoming prevalent. The standardization of lattice-based cryptographic algorithms and the growing awareness of cryptographic migration has led to Post-Quantum Cryptography (PQC) becoming the most prominent mitigation solution for dealing with quantum threats. Digital twins, and autonomous self-healing architectures, are still under-explored. The findings indicate that current research is focused on enhancing the existing cybersecurity mechanisms while future research should focus on fully integrated Quantum AI resilient architectures. The table 2 shows the quantitative summary for the selected studies.

Table 1. Comparative Assessment

Study	Category	Key Finding	Numeric Indicator (Synthetic)
[1]	AI–Quantum Cybersecurity	AI transforms cybersecurity using PQC, AI analytics and quantum resilience.	AI+PQC integrated framework
[2]	AI + PQC for IoT	LSTM, RL and PQC strengthen IoT security against quantum threats.	91–99% detection
[3]	QC–AI Integration	QML and hybrid QC–AI enable optimization across sectors.	Systematic review
[5]	Quantum Cryptography	RSA/ECC vulnerable; ML-KEM, ML-DSA and SLH-DSA recommended.	NIST PQC
[6]	AI–IoT Blockchain	AI enhances IoT, blockchain and quantum cryptography integration.	103 studies
[7]	AI-based Cryptography	Adaptive encryption and neural cryptanalysis improve resilience.	High resilience
[12]	Smart Grid Security	AI-driven IDS and layered smart-grid protection.	Comprehensive review
[24]	Quantum Key Distribution	QKD secures smart-grid communications.	IEEE Access 2025
[15]	Hybrid Encryption	Quantum-resistant hybrid encryption for IoT smart grids.	Hybrid model
[17]	Quantum Digital Twins	Quantum computing enables digital twins and optimization.	Future roadmap
[25]	Secure IoT Smart Grid solutions.	Digital twins, leveraging AI, quantum-secured communications, and CPS–IoT resilience of smart grids.	AI Quantum Digital Twin Framework

Table 2. Quantitative Summary Analysis

Ref	Research Focus	AI	Smart Grid	IoT	Quantum	Main Contribution
[1]	AI & Quantum Cybersecurity	✓	–	–	✓	AI-driven cybersecurity paradigms

[2]	AI + PQC for IoT	✓	–	✓	✓	AI-powered post-quantum IoT security
[5]	Quantum Cryptography	✓	–	–	✓	Strategic migration to quantum-safe cryptography
[12]	Smart Grid Cybersecurity	✓	✓	✓	–	AI-based smart grid protection
[24]	QKD for Smart Grid	–	✓	–	✓	QKD applicability to smart grids
[17]	Quantum Digital Twins	✓	✓	–	✓	Quantum-enabled digital twins

Future Directions:

Future research directions should seek to build cybersecurity frameworks that incorporate Quantum AI integration such as Quantum Machine Learning, Post Quantum Cryptography, Quantum Key Distribution, machine learning, block chain, federated learning, digital twins, and Zero Trust Architecture into more resilient cybersecurity platforms. We need to give more attention to lightweight quantum cryptographic strategies for resource limitation in IoT systems, Explainable Artificial Intelligence (XAI) systems for operational decision support, privacy preserving collaborative learning, and autonomous cyber defence systems that can act in real time to mitigate threats. Moreover, experimental validation is necessary to move from theory to industry deployment, as this requires the use of realistic smart grid testbeds, large-scale benchmark datasets and hardware-in-the-loop simulations.

Conclusion:

The aim of this systematic review was to explore the synergy among Quantum Computing (QC), Artificial Intelligence (AI), and Smart Grid Cybersecurity, with a specific focus on the emerging technologies, the new threats, and the resilient security architectures. The results show that although AI technologies such as intelligent intrusion detection, predictive threat intelligence, anomaly detection, and automated responses for smart grid systems are highly beneficial in terms of enhancing system security, traditional cryptographic algorithms such as RSA and ECC face significant security challenges due to advances in quantum computing of quantum computing. For this reason, Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD) and Quantum Machine Learning (QML) have become a must-have technology to protect the future smart grid. The review also indicates that the architecture of resilient cybersecurity must be multi-layered with the inclusion of Artificial Intelligence, Quantum-secure Cryptography, Block chain, Zero Trust Architecture, Edge Intelligence and Digital Twins to create adaptive and autonomous cyber defense. While there has been great progress, obstacles to overcome include a lack of real-world implementations, limited interoperability, computational complexity, limited standardization of datasets, and a need for scalable quantum-resilient solutions. This review highlights these research gaps and proposes a Quantum-AI Convergence Framework for future research and industrial applications in future research and industrial use. In conclusion, the integration of AI and quantum cybersecurity tools holds great promise for advancing the implementation of safe intelligent, and sustainable smart grid infrastructures that can withstand both conventional and quantum based cyber threats, ensuring the reliability, resilience, and future security of smart grid systems.

Acknowledgment:

The authors are grateful to their respective institutions for the support and assistance they have received in completing this study.

References:

[1] K. Iqbal, S. S. Ali, R. Ali, S. Ali, and B. Raza, “Artificial Intelligence in the Quantum

Era: Transforming Cybersecurity Paradigms," *Annu. Methodol. Arch. Res. Rev.*, vol. 4, no. 4, pp. 469–483, Apr. 2026, doi: 10.66021/.

[2] M. M. Saeed and F. Alqahtani, "AI and post-quantum cryptography powered cybersecurity approaches for IoT systems: a literature review," *PeerJ Comput. Sci.*, vol. 12, 2026, doi: 10.7717/PEERJ-CS.3502/.

[3] V. G. Pineda, A. Valencia-Arias, F. E. L. Giraldo, and E. A. Zapata-Ochoa, "Integrating artificial intelligence and quantum computing: A systematic literature review of features and applications," *Int. J. Cogn. Comput. Eng.*, vol. 7, pp. 26–39, Dec. 2026, doi: 10.1016/J.IJCCE.2025.08.002.

[4] R. Tanveer, "Quantum Computing and Artificial Intelligence Security," May 2026, doi: 10.2139/SSRN.6817998.

[5] V. Mothukuri and R. M. Parizi, "Securing Cryptography in the Age of Quantum Computing and AI: Threats, Implementations, and Strategic Response," Mar. 2026, Accessed: Aug. 15, 2026. [Online]. Available: https://arxiv.org/pdf/2603.06969

[6] K. Adere *et al.*, "A systematic review of artificial intelligence applications in Internet of Things, blockchain, and quantum cryptography," *Discov. Artif. Intell. 2026 61*, vol. 6, no. 1, pp. 270-, Feb. 2026, doi: 10.1007/S44163-026-01029-1.

[7] M. A. Abdewi, F. A. Emara, A. A. Gouda, and M. A. Razek, "AI-Based Cryptography: A Comprehensive Review of Adaptive Encryption, Neural Cryptanalysis, and Post-Quantum Resilience," *Eng. Technol. Appl. Sci. Res.*, vol. 16, no. 2, pp. 33790–33797, Apr. 2026, doi: 10.48084/ETASR.16510.

[8] A. U. R. Butt, M. Asif, M. A. Rasheed, and S. Shafiq, "Quantum-Secure Healthcare: A Comprehensive Review of Post-Quantum Cryptography and Cyber Defense in IoMT," *Int. J. Theor. Appl. Comput. Intell.*, vol. 2026, pp. 132–148, Jun. 2026, doi: 10.65278/IJTACI.2026.67.

[9] W. Rodgers, I. Cenar, and G. O. Gamble, "Quantum-enhanced throughput pathways: Integrating Rodgers' TPM with quantum ethical frameworks for AI-driven cybersecurity," *Acta Psychol. (Amst).*, vol. 263, p. 106231, Mar. 2026, doi: 10.1016/J.ACTPSY.2026.106231.

[10] Z. Damekhaly Turay, M. Koroma, M. Syed Fofanah, and D. Bob Kaitibi, "AI-Driven Cybersecurity In Industry 4.0: A Global Comparative Analysis Of Detection Methods, Challenges, And Resilient Solutions," *Int. J. Adv. Res.*, vol. 14, no. 01, pp. 54–75, Jan. 2026, doi: 10.21474/IJAR01/22515.

[11] A. A. H. Alnaabi and A. A. H. Al Mahruqi, "Artificial intelligence methods for enhancing cybersecurity in Oman: a comprehensive review," *J. Cloud Comput. 2026 151*, vol. 15, no. 1, pp. 48-, Feb. 2026, doi: 10.1186/S13677-026-00860-2.

[12] A. Ali, M. Wadi, and W. Elmasry, "Cybersecurity in Smart Grids and Other Application Fields: A Review Paper," *Energies 2026, Vol. 19, Page 246*, vol. 19, no. 1, p. 246, Jan. 2026, doi: 10.3390/EN19010246.

[13] K. Achuthan, S. Ramanathan, S. Srinivas, and R. Raman, "Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions," *Front. Big Data*, vol. 7, p. 1497535, 2024, doi: 10.3389/FDATA.2024.1497535.

[14] B. Mallick *et al.*, "Quantum-Secure Communication for Future Cyber-Physical and IoT Systems: A Systematic Review of Classical to Learning Approaches," *Comput. 2026, Vol. 15, Page 389*, vol. 15, no. 6, p. 389, Jun. 2026, doi: 10.3390/COMPUTERS15060389.

[15] J. Xiong, L. Shen, Y. Liu, and X. Fang, "Enhancing IoT security in smart grids with quantum-resistant hybrid encryption," *Sci. Reports 2024 151*, vol. 15, no. 1, pp. 3-, Jan. 2025, doi: 10.1038/s41598-024-84427-8.

[16] J. M. Nambundo, O. de Souza Martins Gomes, A. D. de Souza, and R. C. S.

Machado, "Cybersecurity and Major Cyber Threats of Smart Meters: A Systematic Mapping Review," *Energies 2025, Vol. 18, Page 1445*, vol. 18, no. 6, p. 1445, Mar. 2025, doi: 10.3390/EN18061445.
[17] N. Arianne Ornella Lemo, A. M. Saber, D. Kundur, and A. W. Skorek, "Potential of Quantum Computing Applications for Smart Grid Digital Twins and Future Directions," *2025 IEEE PES Conf. Innov. Smart Grid Technol. - Middle East (ISGT Middle East)*, Aug. 2025, doi: 10.1109/ISGTMiddleEast65737.2025.11314205.
[18] M. Cavus, H. Ayan, M. Bell, and D. Dissanayake, "Advances in Energy Storage, AI Optimisation, and Cybersecurity for Electric Vehicle Grid Integration," *Energies 2025, Vol. 18, Page 4599*, vol. 18, no. 17, p. 4599, Aug. 2025, doi: 10.3390/EN18174599.
[19] D. Said, M. Bagaa, A. Oukaira, and A. Lakhssassi, "Quantum Entropy and Reinforcement Learning for Distributed Denial of Service Attack Detection in Smart Grid," *IEEE Access*, vol. 12, pp. 129858–129869, 2024, doi: 10.1109/ACCESS.2024.3441931.
[20] D. Said, "Quantum Computing and Machine Learning for Cybersecurity: Distributed Denial of Service (DDoS) Attack Detection on Smart Micro-Grid," *Energies*, vol. 16, no. 8, pp. 1–11, 2023, Accessed: Aug. 15, 2026. [Online]. Available: https://ideas.repec.org/a/gam/jeners/v16y2023i8p3572-d1128487.html
[21] R. Yan, J. Dai, Y. Wang, Y. Xu, and A. Qun Liu, "Quantum-Key-Distribution Based Microgrid Control for Cybersecurity Enhancement," *Conf. Rec. - IAS Annu. Meet. (IEEE Ind. Appl. Soc.*, vol. 2021-October, 2021, doi: 10.1109/IAS48185.2021.9677160.
[22] T. Alsuwian, A. Shahid Butt, and A. A. Amin, "Smart Grid Cyber Security Enhancement: Challenges and Solutions—A Review," *Sustain. 2022, Vol. 14, Page 14226*, vol. 14, no. 21, p. 14226, Oct. 2022, doi: 10.3390/SU142114226.
[23] T. Berghout, M. Benbouzid, and S. M. Muyeen, "Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects," *Int. J. Crit. Infrastruct. Prot.*, vol. 38, p. 100547, Sep. 2022, doi: 10.1016/J.IJCIP.2022.100547.
[24] W. Grice, M. Olama, A. Lee, and P. G. Evans, "Quantum Key Distribution Applicability to Smart Grid Cybersecurity Systems," *IEEE Access*, vol. 13, pp. 17398–17413, 2025, doi: 10.1109/ACCESS.2025.3533942.
[25] H. Gautam, S. Roy, D. Lakshmi, S. Garg, N. Kassarwani, and N. Nagpal, "Enabling Renewable Power Through Cyber-Physical Systems and Internet of Things in Smart Grids," *Lect. Notes Electr. Eng.*, vol. 1565 LNEE, pp. 307–319, 2026, doi: 10.1007/978-981-95-2149-4_27/SAVE-RESEARCH.