iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VII **Month of publication:** July 2026

DOI: https://doi.org/10.22214/ijraset.2026.84156

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VII July 2026- Available at www.ijraset.com

Post-Quantum Secure Software-Defined Networking for Cloud and Edge Computing

Mr. Ashish Sharma[1], Dr. Upendra Singh[2]
[1]*H.O.D. Computer Science & Engineering, Department of Computer Science & Engineering, Indore Women's Polytechnic College, Indore, India*
[2]*Assistant Professor, Department of Information Technology, Shri G. S. Institute of Technology & Science (SGSITS), Indore, India*

Abstract: ***Conventional cryptographic algorithms that are widely used in Software-Defined Networking (SDN), cloud computing, and edge computing infrastructures are facing a serious challenge because of the fast development of quantum computing. The traditional public-key cryptography like RSA and Elliptic Curve Cryptography (ECC) is believed to be vulnerable to quantum attacks, which will require quantum-resistant security mechanisms to be adopted. The past few years have seen a focus on incorporating Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), Artificial Intelligence (AI), blockchain, and Zero Trust Architecture (ZTA) into SDN, with the aim of creating secure, programmable, and intelligent communication infrastructures. The paper summarizes the recent progress in post-quantum secure SDN in cloud and edge computing. The study starts by examining how lattice-based cryptographic algorithms like CRYSTALS-Kyber and CRYSTALS-Dilithium can be integrated in SDN controllers and SDN programmable networks. Then, hybrid QKD-PQC architectures for quantum-safe communication are discussed, followed by intelligent SDN architectures based on AI-powered threat detection, blockchain-based trust management, and adaptive cryptographic orchestration. Moreover, the paper reviews recent advances, summarizes research challenges, and points towards scalable, autonomous, and quantum-resistant networking infrastructures for next-generation cloud, IoT, edge and 6G networks and ecosystem.***

Keywords: ***Software-Defined Networking, Post-Quantum Cryptography, Quantum Key Distribution, Cloud Computing, Edge Computing, Zero Trust Architecture, Blockchain, Artificial Intelligence, Network Security, 6G Networks.***

I. INTRODUCTION

By breaking the control plane from the data plane, Software-Defined Networking (SDN) has revolutionized today's communication networks into a centralized network intelligence, network programmability, and dynamic management of resources. The architectural flexibility of SDN has led it to become the networking paradigm of choice for cloud computing, edge computing, Internet of Things (IoT), intelligent transportation systems, industrial automation and the new generation of communication networks, known as the sixth generation (6G). SDN simplifies orchestration of the network through centralized controllers, and enhances scalability, traffic engineering and service provisioning.

While SDN has a number of benefits, it also poses substantial security issues, as the centralized-control entity becomes a key point of attack for bad actors. RSA and Elliptic Curve Cryptography (ECC) are mainly used to secure communication between controllers and forwarding devices in existing SDN deployments. But these cryptographic systems are not sustainable in the future due to quantum computing's acceleration. In the presence of a practical quantum computer, quantum algorithms like Shor's algorithm can easily break classical public-key encryption, which will make most secure communication channels insecure.

In response, researchers have introduced Post-Quantum Cryptography (PQC), which are mathematical problems that are resistant to quantum computers, including lattice-based cryptography, code-based cryptography, and hash-based signatures. Algorithms such as key encapsulation with CRYSTALS-Kyber and digital signatures with CRYSTALS-Dilithium have recently been standardized and are emerging as basic components for developing secure communication systems in the future. Meanwhile, Quantum Key Distribution (QKD) is another information-theoretic security method that takes advantage of quantum mechanical properties to provide secure key exchange, ensuring security even against quantum threats.

In addition to cryptographic security, current secure SDN architectures are increasingly leveraging Artificial Intelligence (AI), blockchain, Zero Trust Architecture (ZTA), programmable data planes, and crypto-agile key management in order to deliver intelligent threat detection, decentralized trust, adaptive access control, and automated security policy enforcement. These technologies work together to improve the resilience of cloud-edge infrastructures, and to enable autonomous network management.

©IJRASET: All Rights are Reserved

In this paper, the authors summarize the latest progress in the field of post-quantum secure SDN in cloud and edge computing, covering the state of the art in PQC-enabled SDN architectures, hybrid PQC-QKD communication infrastructure, and intelligent AI-based secure networking solutions. The paper also highlights the challenges and opportunities in the continued research for achieving scalable, programmable, and quantum-resilient network infrastructure.

II. LITERATURE REVIEW

A. *Post-Quantum Cryptography for Software-Defined Networking*

Modern, quantum computers are making traditional public-key cryptography (PKC) algorithms like RSA and ECC increasingly insecure, raising the need for post-quantum cryptography (PQC) in the future Software-Defined Networking (SDN) world. The past few years have seen the growth of research on the incorporation of lattice-based cryptographic methods such as CRYSTALS-Kyber and CRYSTALS-Dilithium in the SDN control and data planes in order to establish quantum-resistant communication channels. Bhargavan et al. [1] introduced resilient space communications with a secure SDP with high assurance PQC mechanisms. However, Satish et al. [2] proposed a lightweight cryptographic algorithm called Ascon and Kyber, which is used along with SDN to ensure adaptive security for smart-home IoT devices while reducing latency and energy consumption. Likewise, Mrinal and V [3] explored the deployment of ML-KEM and ML-DSA in SDN and showed that the implementation of PQC in such environment can be performed with key sizes and handshake times that are larger, but still acceptable by employing the secure communication techniques. Kumar et al. [6] introduced a two-phase migration approach that allows SDN infrastructures to move from classical cryptography to PQC without impacting the network services. Their solution dealt with the problem of compatibility and discussed deployment options for hybrid cryptographic environments.

Recent studies also have expanded the adoption of PQC to cloud computing and IoT systems. Kjamilji [5] suggested a secure memory allocation mechanism for post-quantum cloud infrastructures that guarantees the privacy of workloads in the cloud by employing quantum-resistant cryptographic primitive. To secure IOT networks against DDoS, Shanker and Ellapan [11] designed a lightweight authentication mechanism that combines CRYSTALS-Kyber and Dilithium and adaptive traffic filtering based on SDN. Similarly, Sanon and Schotten [17] proposed a centralized cryptographic management framework supporting cryptographic agility for future mobile networks and facilitating smooth transitions into PQC-based 6G networks. Overall these studies highlight the essential role of PQC as the bottom-line security layer in next generation SDN-enabled communication systems, though there are still some open research issues such as computational overhead, interoperability and dynamic key management.

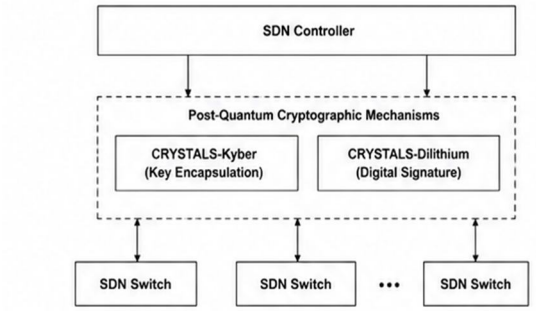


Figure 1. Post-Quantum Cryptography Integration in Software-Defined Networking Architecture

The flow of post-quantum cryptographic mechanisms in Software Defined Networking (SDN) architecture is shown in Figure 1. The SDN controller is responsible for managing secure communication securely, including applying quantum-resistant algorithms like CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures. These cryptographic modules provide an authenticated and confidential communication channel between the controller and SDN switches and ensures the protection of the control plane from future quantum computer attacks, while keeping network management and policy secure.

B. *Quantum Key Distribution and Hybrid Quantum-Safe SDN Architectures*

PQC gives computational security against quantum attacks and Quantum Key Distribution (QKD) gives information-theoretic security by using the principles of quantum mechanics. In this context, studies are growing in the field of hybrid architectures that integrate QKD and PQC in an SDN-based network orchestration framework. To dynamically allocate quantum communication resources, Patil and Mathews [7] proposed an SDN-enabled machine learning framework consisting of quantum communication models which predict optimal paths in the network by implementing Random Forest models based on a Quantum Bit Error Rate

(QBER) and key generation rate. They found that their results showed that their networks were more adaptable and that they were able to use resources securely.

Szymanski [4] proposed an architecture for deterministic Industrial IoT (Det-IIoT) using SDN, Zero Trust Architecture (ZTA), PQC, and symmetric cryptography to support ultra-low latency, quantum safe industrial communication, while maximizing the use of the bandwidth. The security paradox of practical QKD systems was discussed by Szymanski [8] which identified the vulnerabilities due to classical cyber-attacks and proposed an SDN-based deterministic architecture which reduces the information leakage by means of AI-based Zero Trust access control.

The integration of hybrid PQC-QKD has been investigated by several researchers. To achieve secure interoperability between heterogeneous quantum communication infrastructures, Mendez et al. [15] proposed an inter-domain communication framework based on SDN. A multi-hop trusted-node network with scalable end-to-end quantum-safe communication has been proposed by Spooren et al. [14] which includes a layered design of WireGuard tunnels, PQC key exchange based on Rosenpass, and ETSI compliant QKD interfaces. Likewise, V and Avula [13] proposed a crypto-agile Zero Trust design for multi-cloud systems that uses the SDN controller to dynamically choose the session key for QKD or ML-KEM, based on the network conditions. In order to provide security for V2X communication under the strict latency requirements of ITSs, Li et al. [9] proposed a hybrid quantum-safe communication scheme by combining QKD, PQC, and SDN.

Moreover, Mehic et al. [18] discussed DDoS attacks on the key management systems of QKD and developed resilient key allocation strategies to ensure secure communication when resources are exhausted. All these studies show that hybrid PQC-QKD architecture controlled by SDN controllers is one of the most promising avenues to pursue in the development of quantum-resistant communication networks.

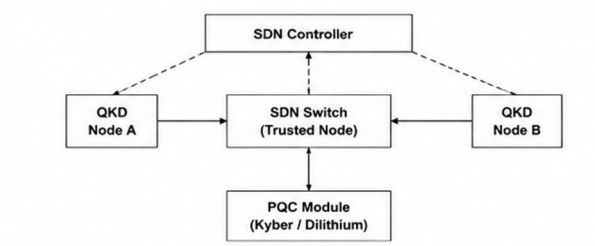


Figure 2. Hybrid Quantum Key Distribution and Post-Quantum Cryptography Enabled SDN Framework

In Figure 2, a hybrid quantum-safe SDN is introduced that integrates Quantum Key Distribution (QKD) with Post-Quantum Cryptography (PQC). The SDN controller dynamically coordinates the operation of the QKD nodes, trusted forwarding devices, and PQC modules to create end-to-end secure communication while maintaining security of the keys. The information-theoretic secure key generation by QKD is compared with computational security in network authentication and encryption by PQC algorithms. This hybrid architecture improves the reliability of communication, its scalability and resilience against classical and quantum cyber threats.

C. Intelligent, Zero-Trust, and Blockchain-Based Secure SDN for Future Networks

In addition to quantum-resistant cryptography, current SDN research has also introduced the concept of artificial intelligence, blockchain, Zero Trust Architecture, and programmable networking in order to create an autonomous and resilient network infrastructure. Rivera et al. [10] came up with an SDN framework that uses CRYSTALS-Dilithium signatures to ensure the authenticity of communication between SDN controllers, and Kyber-based key encapsulation to encrypt the controller communication channels, with smart contracts enabling decentralized verification and secure distribution of public keys. Their work showed that blockchain technology can greatly advance the trust management among distributed SDN controllers. AI has also become an integral part of the intelligent SDN systems. Patil and Mathews [7] used machine learning to improve the adaptability of quantum resources allocation, whereas Szymanski [4,8] introduced AI-based Zero Trust access control into deterministic SDN architectures for reinforcing security of industrial IoT systems against insider and outsider attacks. Chouhan et al. [12] thoroughly reviewed the cybersecurity issues of SDN, NFV, network slicing, and massive IoT for 5G and 6G networks and noted that future communication systems need to have integrated security solutions that involve federated learning, blockchain-based security, secure orchestration, post quantum cryptography, and AI-based threat detection.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

The evolution of intelligent secure networking is further exemplified with emerging applications. In order to grant interoperability and keep the implementation complexity down, Roşu and Graur [19] proposed minimal post-quantum certificate profiles for federated space communication infrastructures. Torres-Figueroa et al. [16] showed experimentally that the randomized identification scheme is semantic secure for post quantum wireless communication. The developments suggest a decentralized trust management will be more and more used in future SDN architectures, as well as a programmability of security policies, automation through AI tools, and a crypto-agile approach will be necessary to meet the security needs of cloud, IoT, satellite, intelligent transportation and upcoming 6G networks.

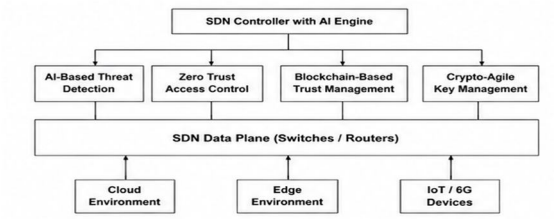


Figure 3. Intelligent Zero-Trust and Blockchain-Based Secure Software-Defined Networking Architecture

The Figure 3 illustrates an intelligent SDN architecture that incorporates and combines Artificial Intelligence (AI), Zero Trust Architecture (ZTA), blockchain technology and crypto-agile security mechanisms. The SDN controller uses Artificial Intelligence (AI) threat detection, continuous identity verification, blockchain-based decentralized trust management and adaptive cryptographic policy enforcement to secure cloud, edge, IoT and next generation 6G environments. This allows for independent security control, adaptable access rights, secure key management, and resilient protection against advanced cyber and quantum attacks, along with extensible and programmable network architectures.

D. Research Gap

Despite great strides in the combination of Post-Quantum Cryptography, Quantum Key Distribution, blockchain, Zero Trust Architecture, and AI in SDN, the majority of previous research has examined these technologies individually or in certain isolated sets. It is rare to find an architecture that includes AI-driven intelligent threat detection, adaptive SDN orchestration, hybrid PQC-QKD key management, blockchain-based decentralized trust, and Zero Trust access control all in one. In addition, robust solutions that can also serve cloud-edge environments, multi-domain SDN, 6G networks, and resource-constrained IoT systems that are low latency and scalable are lacking. Such restrictions pave the way for developing a uniform intelligent quantum-secure SDN framework that provides adaptive, scalable and end-to-end resilient communication for future network infrastructures.

Table 1. Systematic Literature Review of Recent Post-Quantum Secure SDN Research (2022–2026)

Ref.	Author(s) & Year	Proposed Work	Methodology / Technology	Key Findings	Limitation
[1]	Bhargavan et al. (2025)	Secure satellite SDN payload	Post-Quantum Cryptography (PQC)	Improved secure satellite communication against quantum threats	Limited evaluation in terrestrial SDN
[2]	Satish et al. (2025)	FEC-SDNShield	SDN + Ascon + CRYSTALS-Kyber + Device Fingerprinting	Reduced latency, energy consumption and memory overhead for IoT	Focused only on smart-home IoT
[3]	Mrinal & V (2025)	PQC performance analysis in SDN	ML-KEM, ML-DSA	Demonstrated feasibility of PQC deployment in SDN	Larger key sizes increase handshake delay
[4]	Szymanski (2026)	Deterministic Industrial IoT	SDN + AI + Zero Trust + PQC	Achieved ultra-low latency and high bandwidth utilization	Complex deployment in large-scale environments

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[5]	Kjamilji (2026)	Secure cloud memory allocation	Quantum-resistant cryptographic primitives	Improved cloud privacy and secure memory management	Focus limited to cloud infrastructure
[6]	Kumar et al. (2025)	PQC migration framework	Hybrid cryptography for SDN	Smooth transition from classical to quantum-safe networks	Lacks implementation in heterogeneous SDN
[7]	Patil & Mathews (2026)	Intelligent QKD resource allocation	SDN + Machine Learning + QKD	Adaptive routing and secure quantum key allocation	Evaluated mainly in simulated environments
[8]	Szymanski (2026)	Quantum-safe Deterministic IIoT	AI + Zero Trust + SDN + PQC	Improved resilience against cyber attacks in QKD networks	High implementation complexity
[9]	Li et al. (2026)	QuanReS Framework	SDN + QKD + PQC for V2X	Low-latency secure communication for intelligent transportation	Specific to V2X scenarios
[10]	Rivera et al. (2025)	Secure inter-controller communication	Blockchain + Kyber + Dilithium	Decentralized trust and secure SDN controller communication	Increased blockchain overhead
[11]	Shanker & Ellapan (2026)	PQC-enabled DDoS mitigation	Kyber + Dilithium + SDN	Lightweight authentication with adaptive DDoS defense	Performance under large-scale attacks not evaluated
[12]	Chouhan et al. (2026)	Review of 5G/6G SDN security	SDN, NFV, AI, PQC, Blockchain	Comprehensive survey of future network security	Review article without proposed framework
[13]	V & Avula (2025)	Multi-cloud Zero Trust architecture	SDN + PQC + QKD + P4	Crypto-agile key orchestration for cloud environments	Prototype-level implementation
[14]	Spooren et al. (2026)	Layered QKD-PQC architecture	WireGuard + Rosenpass + PQC	Scalable end-to-end quantum-safe communication	Trusted-node dependency
[15]	Mendez et al. (2024)	Hybrid quantum-safe SDN domains	SDN + Hybrid QKD/PQC	Secure inter-domain communication using SDN	Limited cross-domain scalability evaluation
[16]	Torres-Figueroa et al. (2025)	Semantic secure identification	Randomized Identification + SDR	Enhanced semantic security for wireless communication	Not specifically designed for SDN
[17]	Sanon & Schotten (2025)	Cryptographic Management Function	Software-defined cryptography + PQC	Dynamic cryptographic agility for 5G/6G	Implementation complexity
[18]	Mehic et al. (2022)	Secure QKD key management	SDN + QKD	Mitigated DoS attacks on QKD key management	Limited to QKD infrastructure
[19]	Roşu & Graur (2025)	Federated Space PKI	Post-Quantum Certificates (C509)	Reduced certificate complexity for space networks	Limited practical deployment

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

The past few years of research and publication have revealed a clear progression in the definition of SDN security to quantum-resilient intelligent networking. Previous research has concentrated on embedding Post-Quantum Cryptography (PQC) in SDN controllers and communication paths and the more recent literature investigates the use of Quantum Key Distribution (QKD), Artificial Intelligence (AI), Zero Trust Architecture (ZTA), Blockchain and crypto-agile key management to build secure, adaptive and autonomous networking frameworks. Current methods tend to focus on these technologies in isolation or in small clusters, however. An important research gap is the integration of AI-driven threat intelligence, hybrid PQC-QKD key management, blockchain-based trust, and Zero Trust access control, along with SDN orchestration, in the cloud-edge, IoT, and future 6G networks

III. METHODOLOGY

The processes in this review paper are derived from the systematic literature analysis methodology to explore recent advances in post-quantum secure SDN in Cloud Computing and Edge Computing. First, the IEEE Xplore, Springer, ACM Digital Library, Elsevier ScienceDirect and other peer-reviewed publications published from 2022 to 2026 were gathered. Most of the keywords searched were Post-Quantum Cryptography (PQC), Software-Defined Networking (SDN), Quantum Key Distribution (QKD), Cloud Computing, Edge Computing, Blockchain, Zero Trust Architecture, and Artificial Intelligence.

Following the elimination of duplicate and irrelevant publications, nineteen high-quality research papers were chosen based on relevance, novel techniques, implementation methodology and their role in advancing quantum-secure SDN. The research studies selected were systematically grouped into three main themes of research.

The first category examines the possibility of incorporating Post-Quantum Cryptography in SDN architectures, focusing on lattice-based solutions, secure controller communications, lightweight authentication methods, and transitions from classical cryptography.The first category explores how to incorporate Post-Quantum Cryptography in SDN architectures, including lattice-based solutions, secure controller communications, lightweight authentication methods, and transitions from classical cryptography. The second class of works are dedicated to hybrid Quantum-safe communication systems, which integrate QKD and Post-Quantum Cryptography techniques and SDN orchestration, in order to enable secure key management and trusted communication channels. The third category looks at the intelligent SDN architecture which includes the integration of Artificial Intelligence, blockchain technology, Zero Trust Architecture, crypto-agile security and programmable networking for autonomous Cyber Defense.

The architectures, cryptographic techniques, security mechanisms, performance properties, application field, benefits and research drawbacks of each publication were analysed. Lastly, comparative analysis revealed current trends, gaps in existing research, and promising research directions for scalable and quantum resistant cloud-edge network infrastructures.

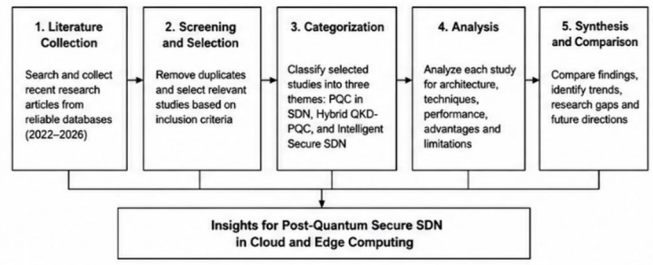


Figure 4. Systematic Research Methodology for Post-Quantum Secure Software-Defined Networking

The systematic methodology which was used in this study is shown in Figure 4. The process starts with literature search from the scientific reputed data sources and then screening and selection of relevant literature. The publications selected are classified according to the major research themes, analysed in terms of their methodology and contribution, and finally synthesised to identify current trends, research gaps and future research directions for post-quantum secure SDN for cloud and edge computing.

IV. APPLICATIONS AND ADVANTAGES

A. Applications

Post quantum secure SDN architectures possess wide applicability in next generation communication infrastructures. They enable distributed data centers to communicate securely in cloud computing systems without being susceptible to quantum attacks, and in virtualization, workload migration and resource orchestration. In edge computing, they facilitate low latency and low computing load between edge servers, IoT gateways and edge devices, and provide secure communication between them.

The applications of Industrial Internet of Things (IIoT) find its value in secure deterministic communication, intelligent manufacturing and autonomous process control. These architectures are used in smart city infrastructures to defend the intelligent transportation system, surveillance networks, smart grids, and public safety applications from future quantum threats. In healthcare, confidential transmission of electronic medical records, telemedicine services, and medical IoT communications are made possible by post-quantum secure SDN. Crypto-agile SDN infrastructures can be used to enable secure digital banking, blockchain services, and transaction processing in financial institutions. Programmable security, network slicing protection, and dynamic management of cryptographic keys are key advantages of emerging 5G and 6G communication networks. Additionally, there is an increasing need for quantum-resistant communication with SDN orchestration in satellite communication systems, defense networks, autonomous vehicles, and aerospace infrastructures.

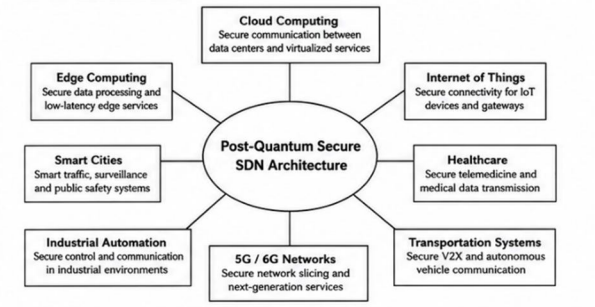


Figure 5. Application Domains of Post-Quantum Secure Software-Defined Networking

Major application areas of post-quantum secure SDN is shown in Figure 5. The architecture enables secure cloud, edge, Internet of Things (IoT), industrial automation, healthcare systems, intelligent transportation, smart cities and 5G/6G communication networks. These applications include programmable networking, quantum resistance, centralized security management and reliable service delivery.

B. Advantages

Incorporating post-quantum cryptography techniques into SDN can offer a host of benefits over traditional secure networking methods. Quantum-resistant cryptographic algorithms not only enhance long-term security against quantum computing attacks but they are also compatible with programmable network infrastructures. Centralized SDN controllers allow dynamic policy enforcement, key management and fast deployment of cryptographic updates across the network.

Hybrid PQC-QKD architectures enhance confidentiality by leveraging computational security along with information-theoretic secure key exchange. AI boosts network resilience with intelligent intrusion detection, anomaly detection, predictive traffic analysis, and automated cyber-defense. A blockchain solution provides distributed SDN controllers with decentralized trust and blocks unauthorized changes to the policy. Zero Trust Architecture is constantly authenticating users, devices, and applications to decrease insider risks and unauthorized access. Cryptographic agile frameworks help to move from one cryptographic algorithm to another without any disruption in service, which will make the process of rolling out to a future algorithm much easier. In sum, these technologies enhance network privacy, security, integrity, availability, scalability, programmability, and resilience in cloud-edge computing environments.

V. CONCLUSION AND FUTURE WORK

A. Conclusion

The SDN, when implemented using the post-quantum secure approach, is a promising path for securing future cloud and edge computing systems from the threats posed by a quantum world. The recent developments have already shown that PQC, QKD, AI, Blockchain and ZTA can greatly improve the security, scalability and programmability of SDN environments. From the reviewed studies, it can be seen that significant advances have been made in secure controller communication, adaptive cryptographic control, intelligent detection of threats, and decentralized trust and resilient cloud-edge networking. While some investigations have focused on each security mechanism separately, only a few have attempted to integrate these technologies into a unified and quantum-resistant SDN architectures. As a result, post-quantum secure SDN will be a key ingredient of the future cloud, IoT, industrial automation, and 6G communication systems.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

B. Future Work

Research is needed to develop a single SDN architecture that integrates Post-Quantum Cryptography, Quantum Key Distribution, Artificial Intelligence, blockchain technology, Zero Trust Architecture, and programmable networking. The lightweight post quantum cryptographic algorithms for resource-constrained devices in IoT and edge devices need to be further optimized to reduce the computational overhead. Another direction of potential research interest is AI-controlled autonomous SDN controllers that can predict threats, heal the network automatically, and manage cryptographic protocols dynamically. Multi-cloud interoperability, distributed controller security, programmable data plane with P4 and eBPF, digital twin-based security validation, and secure network slicing for the 6G environment are also worthy of being explored in future work. Finally, significant experimental validation with real deployments on the cloud-edge and the use of standard platforms for benchmarking will be crucial for speeding up the practical deployment of quantum-resilient Software-Defined Networking.

REFERENCES

[1] K. Bhargavan, T. Gazagnaire, F. Kiefer and V. Robles, "Secure Satellite Software-Defined Payloads With High-Assurance Post-Quantum Cryptography," 2025 Security for Space Systems (3S), Noordwijk, Netherlands, 2025, pp. 1-5.

[2] E. G. Satish, B. V. S. Mounika, A. Anand, A. Kumar Pamidi Venkata and G. Chandrashekar, "Adaptive Sdn-Based Lightweight Cryptographic Framework for Post-Quantum Secure Smart Home Iot Networks," 2025 2nd International Conference on Software, Systems and Information Technology (SSITCON), Tumkur, India, 2025, pp. 01-08, doi: 10.1109/SSITCON66133.2025.11342081.

[3] K. Mrinal and V. S, "Performance Analysis of Post-Quantum Cryptographic Algorithms in Software-Defined Networks," 2025 9th International Conference on Computing, Communication, Control and Automation (ICCCBEA), Pune, India, 2025, pp. 1-6, doi: 10.1109/ICCUBEA65967.2025.11283923.

[4] T. H. Szymanski, "Demonstration of an Ultra-Low Latency Secure Deterministic Industrial Internet of Things (IIoT)," 2026 IEEE 23rd Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2026, pp. 1-4, doi: 10.1109/CCNC65079.2026.11366616.

[5] A. Kjamilji, "Secure, Private and Fast Memory Allocation of Processes in Post-Quantum Clouds," 2026 International Seminar on Intelligent Business and Edge-Computing Research (ISIBER), Jakarta, Indonesia, 2026, pp. 587-592, doi: 10.1109/ISIBER68248.2026.11470091.

[6] O. Kumar, D. Rai and S. Badotra, "A Framework for Seamless Transition to Post-Quantum Security in SDN," 2025 2nd Global AI Summit - International Conference on Artificial Intelligence and Emerging Technology (AI Summit), Noida, India, 2025, pp. 1621-1626, doi: 10.1109/AISummit66170.2025.11410753.

[7] C. Patil and L. Mathews, "Software Defined Networking (SDN)-Enabled Machine Learning Approach for Resource Allocation in Quantum Key Distribution Networks," 2026 International Conference on Next-Gen Quantum and Advanced Computing: Algorithms, Security, and Beyond (NQComp), Bangalore, India, 2026, pp. 124-130, doi: 10.1109/NQComp68334.2026.11497741.

[8] T. H. Szymanski, "A Cybersecurity Paradox on Quantum Key Distribution (QKD) and a Deterministic Industrial Internet of Things (IIoT) with AI-based Zero Trust," 2026 IEEE 23rd Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2026, pp. 1-8, doi: 10.1109/CCNC65079.2026.11366320.

[9] S. Li, Y. Xie and M. Iqbal, "QuanReS: A Hybrid Quantum-Enabled Resilient and Secure V2X Communications Framework in Smart Cities," in IEEE Transactions on Consumer Electronics, vol. 72, no. 2, pp. 3940-3948, May 2026, doi: 10.1109/TCE.2025.3647004.

[10] J. José Díaz Rivera, R. Vilalta, R. Muñoz, P. Alemany and L. G. Renom, "Leveraging PQC and Blockchain for Secure and Verifiable SDN Controller Communication," 2025 IEEE 11th International Conference on Network Softwarization (NetSoft), Budapest, Hungary, 2025, pp. 567-572, doi: 10.1109/NetSoft64993.2025.11080638.

[11] S. Shanker and M. Ellapan, "A Post-Quantum Cryptographic Framework for Securing DDoS Mitigation in IoT-Driven Networks," 2026 International Conference on Intelligent Computing, Networks, and Security (IC-ICNS), Bhubaneswar, India, 2026, pp. 1-6, doi: 10.1109/IC-ICNS68863.2026.11537825.

[12] B. Chouhan, A. Sharma, H. Pathak, R. Raj, A. Gopi and A. P. Joshi, "A Comprehensive Review of Cybersecurity in 5G and 6G Networks: SDN, NFV, Slicing, and Massive IoT Security," 2026 13th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2026, pp. 1-7, doi: 10.23919/INDIACom70271.2026.11526205.

[13] V. H and S. R. Avula, "Crypto-Agile Zero-Trust Access for Multi-Cloud via SDN, with PQC-QKD Key Orchestration," 2025 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), Kolhapur, India, 2025, pp. 1-5, doi: 10.1109/ICBDS67396.2025.11377845.

[14] P. Spooren, A. Neuhold, S. Ramacher and T. Hühn, "PQC-Enhanced QKD Networks: A Layered Approach," 2026 International Conference on Quantum Communications, Networking, and Computing (QCNC), Kobe, Japan, 2026, pp. 354-358, doi: 10.1109/QCNC69040.2026.00060.

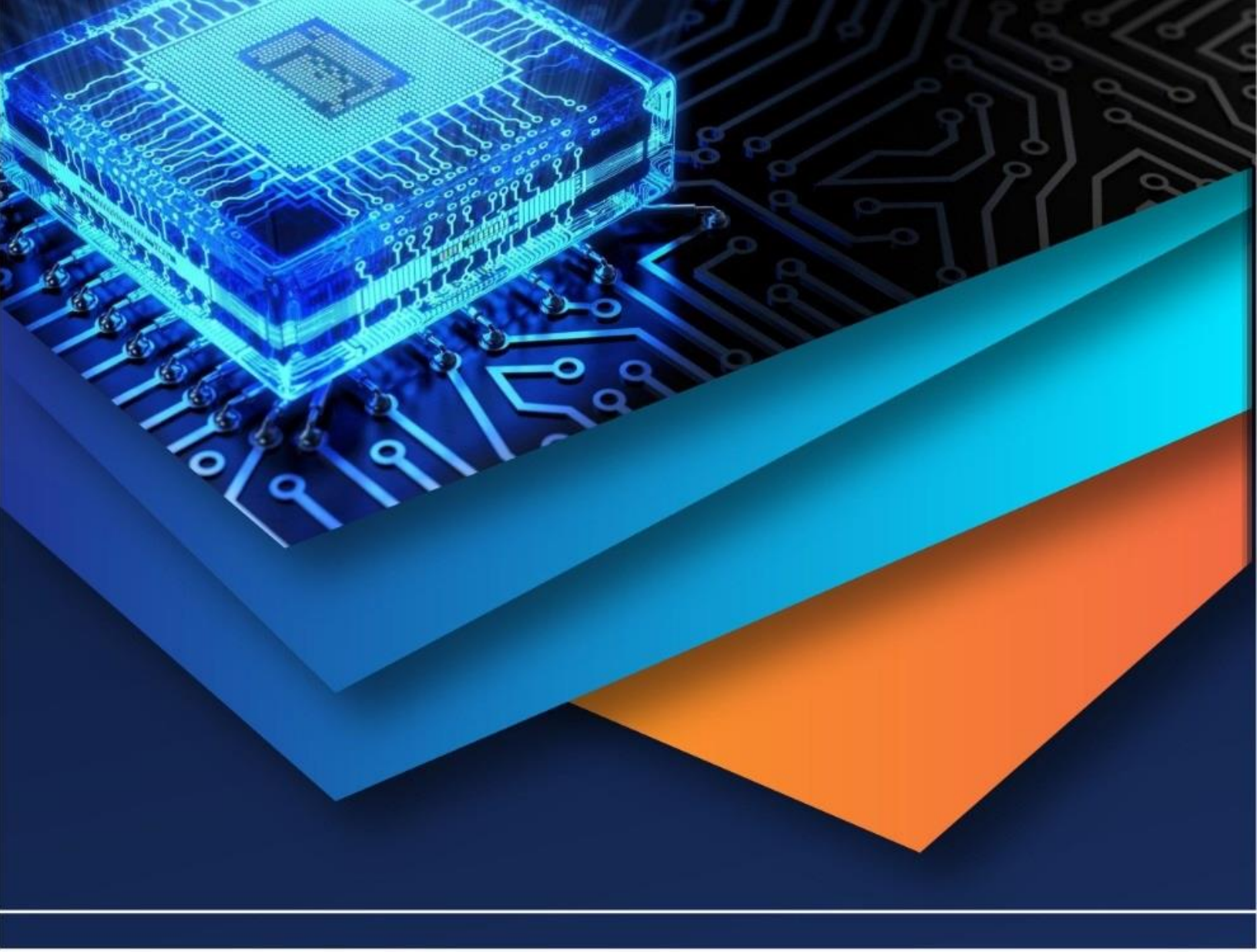
[15] R. B. Mendez et al., "SDN-Based Hybrid Quantum-Safe Domain Intercommunication Within MadQCI," 2024 International Conference on Quantum Communications, Networking, and Computing (QCNC), Kanazawa, Japan, 2024, pp. 168-175, doi: 10.1109/QCNC62729.2024.00034.

[16] L. Torres-Figueroa et al., "Experimental Analysis of Semantic-Secure Randomized Identification in AWGN Channels," GLOBECOM 2025 - 2025 IEEE Global Communications Conference, Taipei, Taiwan, 2025, pp. 4662-4668, doi: 10.1109/GLOBECOM59602.2025.11431815.

[17] S. P. Sanon and H. D. Schotten, "Quantum-Ready Mobile Communications: Cryptographic Agility for Mobile Networks in the Quantum Era," 2025 IEEE 26th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Fort Worth, TX, USA, 2025, pp. 287-292, doi: 10.1109/WoWMoM65615.2025.00056.

[18] M. Mehic, S. Rass, E. Dervisevic and M. Voznak, "Tackling Denial of Service Attacks on Key Management in Software-Defined Quantum Key Distribution Networks," in IEEE Access, vol. 10, pp. 110512-110520, 2022, doi: 10.1109/ACCESS.2022.3214511.

[19] A. -P. Roşu and O. -A. Graur, "Towards Minimal Certificates for Federated Space Public Key Infrastructure," 2025 Security for Space Systems (3S), Noordwijk, Netherlands, 2025, pp. 1-12.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)