International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 10 October 2026
Page No: 5625-5633
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0735

Next-Generation Cybersecurity for Quantum-Safe Satellite Data:Post-Quantum Cryptographic Framework and Advanced Algorithms

Veena N D [1], Anithadevi M D[2], Kantharaju[3]
[1]Research Scholar, Dept. of Computer Science Engineering, Sri Siddhartha Institute of Technology, Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India
[2]Research Supervisor, Dept. of Electronics and Communication Engineering, Sri Siddhartha Institute of Technology, Sri Siddhartha Academy of Higher Education,Tumakuru, Karnataka, India.
[3]Assistant Professor, Dept. of Bio Medical Engineering, Sri Siddhartha Institute of Technology, Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India.
Emails: *veena.devaraju@gmail.com[1], anithadevimd@ssahe.edu.in[2], kantharaju@ssahe.edu.in[3]*
Orcid: 10009-0003-0020-2219[1], 20009-0007-4483-9181[2],3 0009-0002-0480-4500[3]

Abstract
Conventional cryptographic mechanisms in satellite communication systems are facing great challenges due to the swift progress of quantum computing. Current methods like RSA are quantum vulnerable and there is a pressing need for quantum secure cybersecurity. In this study, the authors suggest a new cyber security framework for secure satellite data transmission with the help of the post-quantum cryptographic methods and intelligent cyber threat detection mechanisms. The proposed approach consists of the following three components: (1) quantum-resistant key generation and encryption using CRYSTALS-Kyber, (2) authentication of digital signatures using CRYSTALS-Dilithium, and (3) an Intrusion Detection System (IDS) based on a Deep Neural Network (DNN) designed for detecting cyberattacks in real time. An additional Quantum Resistance Score (QRS) model also is integrated to assess security robustness against quantum threats. Experimental results show that Kyber obtains efficient encryption and decryption times of 22 µs and 30 µs, respectively, while the size of the ciphertext is compact, at 1,088 bytes. The DNN model attained 98.7% accuracy, 98.2% precision, 97.9% recall, and 98.0% F1-score. The framework resulted in a 96% QRS, attack detection rates of more than 96.9% and throughput of 95 Mbps. The results show that the framework can securely, efficiently and quantum resistively protect next-generation satellite communication systems.
Keywords: *Post-Quantum Cryptography (PQC), Quantum-Safe Satellite Communication, CRYSTALS-Kyber, CRYSTALS-Dilithium, Deep Neural Network (DNN), Quantum Cybersecurity Framework.*

1. Introduction
Satellite communication technologies have made great strides over the last few decades, bringing about a revolution in the digital world that includes global communications, Earth observation, navigation, remote sensing, defence use, environmental monitoring, and broadband communication services [1]. With the growing integration of satellite networks with other critical infrastructures, data security while transmitting and storing data has become a significant concern. Satellite systems constantly share large volumes of critical data on the dispersed networks, which makes them appealing targets for cyberattacks [2]. Classical cryptographic algorithms, like RSA, Diffie–Hellman, “Elliptic Curve Cryptography (ECC)”, have been used traditionally to secure satellite communications for confidentiality, integrity, authentication and non-repudiation [3]. These cryptographic techniques have worked well against traditional computational attacks, but now with the advent of quantum computer, there is a paradigm shift which poses a security threat to the current satellite communication architectures [4]. Additionally, the quantum computer may be able to tackle difficult mathematical puzzles that are beyond the capabilities of a traditional computer. For instance, Shor's algorithm may break popular public-key cryptography schemes and solve discrete logarithm and integer factorization problems in polynomial time [5]. Therefore, the availability of full-scale

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 10 October 2026
Page No: 5625-5633
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0735

quantum computers could jeopardize existing satellite communication encryption techniques [6]. The "harvest now, decrypt later" strategy, which calls for attackers to intercept and store satellite communications now and decrypt them later when satellite have access to quantum computers, exacerbates the problem. For military, political, scientific, and commercial satellite systems that need to offer long-term security of sensitive data and confidentiality, the vulnerabilities are especially troublesome [7]. As shown in Figure 1 Quantum-Secure Satellite Communication Framework.

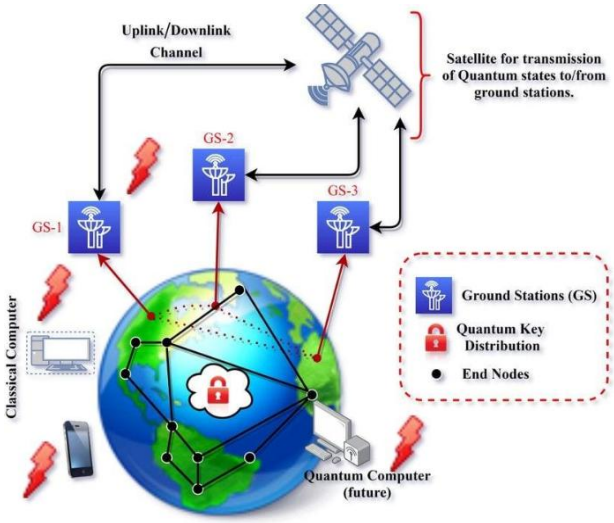


Figure 1 Quantum-Secure Satellite Communication Framework [8]

Researchers and cybersecurity experts are working on new cryptographic algorithms to tackle these new challenges, known as “Post-Quantum Cryptography (PQC)”. Moreover, PQC does not require special hardware or infrastructure, unlike “Quantum Key Distribution (QKD)”, and thus is a realistic solution for satellite communication [10]. Lately, there have been significant advances in lattice-based cryptography, code-based cryptography, hash-based signatures, multivariate polynomial cryptography, and isogeny-based cryptographic schemes, which have shown promising features to provide a quantum-resistant security. Additionally, there has been a recent push towards the standardization protocols that enable secure implementation of post-quantum algorithms for next generation communication systems [11]. The research investigates a future-proof cybersecurity system for satellite data protection that combines post-quantum cryptographic methods with state-of-the-art security algorithms [12]. The concept is to secure data transfer, strengthen authentication mechanisms, improve key management, adaptively identify threats, and defend against quantum-powered cyberattacks [13]. It mitigates the weaknesses of traditional security methods and utilizes new technologies such as post-quantum methods to improve satellite data confidentiality, integrity, and availability in future communication networks [14]. The rest of this paper is organized as follows. In Section 2 the existing literature is reviewed on satellite cyber security and Post Quantum Cryptography. The proposed quantum safe cyber security framework and advanced algorithmic design is presented in Section 3. The methodology and implementation strategy used for the development of the system is described in section 4. The experimental results and performance evaluation are discussed in section 5. Lastly, Section 6 wraps up the paper and future research directions for quantum-resilient satellite communication systems are summarized.

- To develop a quantum-safe cybersecurity framework for protecting satellite data against classical and quantum cyber threats.
- To integrate post-quantum cryptographic algorithms for secure authentication, encryption, and key exchange in satellite communication systems.
- To design advanced security algorithms that optimize computational efficiency, communication performance, and resource utilization in satellite environments.
- To evaluate the security, scalability, and effectiveness of the proposed framework through comprehensive performance and threat-resilience analysis.

2. Literature Review

There have been substantial advances in literature for quantum-safe cybersecurity architectures of satellite communication system and next-generation digital infrastructures. Kosari et al. (2026) [15] introduced a multi-layer security approach for CubeSat networks,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 10 October 2026
Page No: 5625-5633
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0735

combining physical-layer protection, lightweight encryption, and the use of AI for threat detection and prevention to address spoofing and eavesdropping attacks. Dhingra et al. (2026) [16] proposed an adaptive cryptographic framework that integrates PQC, QKD, and AI to boost the agility and security of cryptographic key management. Ali et al. (2025) [17] presented an AI–Quantum cybersecurity architecture that increased the accuracy of threat detection by 96.1% and reduced the latency of detection by 47%. In Boullosa et al. (2025), reseracher have introduced the Q-SATLang framework for autonomous satellite operation, which achieved a response time of 40 ms and an operational availability of more than 99.98% [18]. In conclusion, the various studies demonstrate the potential of combining AI with quantum-resistant technologies to enhance the security of satellite communication systems in the face of new cyber threats. Reddy et al. [19] designed the QuantumShield-BC framework, which enables a throughput of more than 7000 transactions per second and prevents any effectiveness of attack using Sybil attacks, and boosts quantum based attacks resistance. Chandrasekar et al. (2025) [20] proposed the Quantum-Resilient Hybrid Cryptographic Protocol that achieves an efficient security-communication trade-off in low-latency networks. The need for the shift from classical to NIST approved post quantum cryptographic algorithms has been highlighted by Ahmed et al. (2024) [21] and Rawal et al. (2024) [22]. Szymanski et al. (2024) [23] proved the effectiveness of FPGA based quantum-safe architectures in ultra-reliable communication and in reducing denial of service attacks. García-Cid et al. (2024) [24] tested post-quantum migration solutions in Smart Grids, 5G networks and distributed ledgers while Kashiv et al. (2024) [25] demonstrated how AI-driven quantum-resistant SD-WAN architectures boost routing efficiency, flexibility, and overall network security. More research also validated the use of quantum-safe technologies in cloud, enterprise and satellite environments. The need for post-quantum PKI systems for future cybersecurity readiness was emphasized by Hoang et al. (2023) [26]. Kumar et al. (2023) [27] presented the application of quantum satellites and UAV-based communication networks in secure data transmission. Vidaković et al. (2023) [28] compared the standardized post-quantum signature algorithms and found that Dilithium is appropriate for low-power applications, Falcon is able to verify the signature faster and SPHINCS+ is more secure. The future-proof data center security is illustrated by Jain et al. (2023) [29] on the importance of quantum key distribution. In fact, according to authors of the above papers [30, 31, 32], lattice-based, code-based, McEliece and NTRU cryptographic schemes are very resistant to quantum attacks. In general, the papers examined show that PQC, QKD, and intelligent cybersecurity are set to become a viable basis for the creation of secure, scalable, and future-oriented satellite communication systems. While a number of existing studies have proved the security and effectiveness of post quantum cryptography, quantum key distribution, security mechanisms based on artificial intelligence, and security mechanisms based on the distributed ledger blockchain technology, these studies are dedicated to each new security functionality separately. The incorporation of CRYSTALS-Kyber, CRYSTALS-Dilithium, Deep Neural Network-based intrusion detection system, and risk assessment of quantum attack in satellite communication environment has not been studied at any great length. Moreover, the need for an integrated quantum-safe cybersecurity framework is not adequately addressed as comprehensive testing of quantum resistance, communication efficiency, scalability, and real-time cyber-attack detection of next-generation satellite networks are yet to be done.

3. Research Methodology

The research method is to create a quantum-safe cybersecurity framework for satellite communication (SatCom) systems by combining the CRYSTALS-Kyber key encapsulation, the CRYSTALS-Dilithium digital signatures, the Deep Neural Network (DNN)-based intrusion detection, and quantum attack risk assessment. The framework provides a safe and secure way to transmit data, offers strong authentication methods, offers intelligent threat detection, and is designed to withstand new cyber threats resulting from quantum computing. The framework of proposed Work is shown in figure 2.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 10 October 2026
Page No: 5625-5633
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0735

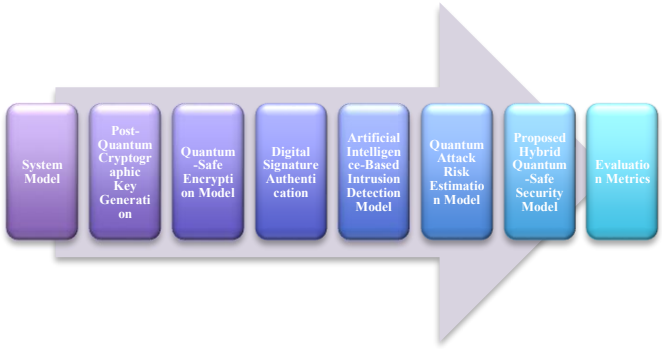


Figure 2 Framework of proposed Work

3.1.System Model

The proposed quantum-safe satellite communication system comprises a network of satellite nodes and a ground station that are linked by secure communication channels. Let the satellites network be denoted by:

$$S = \{S_1, S_2, S_3, \dots, S_n\} \quad (1)$$

where (Si) denotes the (ith) satellite node, (n) represents the total number of satellites, and (G) denotes the ground station. (D) are the data packets made by the satellite. Secure communication between a satellite and the ground station is established using a post-quantum cryptographic key as:

$$C = S_i, G, K_{PQC} \quad (2)$$

where (KPQC) represents the quantum-resistant encryption key generated using post-quantum cryptographic algorithms. This model provides for the confidentiality, integrity, authentication, and defence against classical and quantum computing-related cyberattacks during the data transmission via the satellite.

3.2.Post-Quantum Cryptographic Key Generation

The suggested framework uses the CRYSTALS-Kyber lattice-based key encapsulation mechanism to protect satellite communications against future quantum computing attacks. Firstly, a public random matrix is created:

$$A \in Z_q^{n \times n} \quad (3)$$

where (q) denotes the modulus and (n) represents the lattice dimension. A secret vector and an error vector are sampled from a predefined noise distribution (χ):

$$s \leftarrow \chi^n \quad (4)$$

$$e \leftarrow \chi^n \quad (5)$$

The public key is then computed using the Learning with Errors (LWE) principle:

$$pk = As + e \quad (6)$$

While the private key is defined as:
The key pair (pk,sk) provides a quantum-resistant cryptographic basis that guarantees a secure key exchange, authenticity, and resistance to classical and quantum cryptanalytic attacks in satellite communication networks. As shown in Figure 3 CRYSTALS-Dilithium Signature Generation and Verification Process.

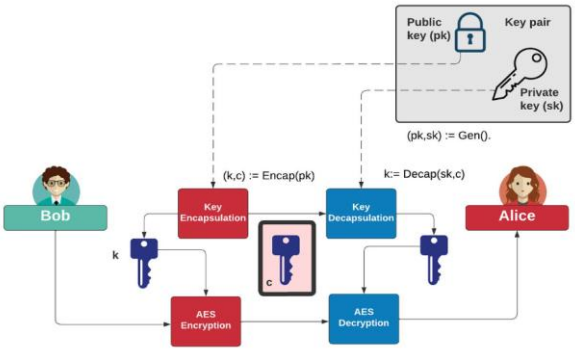


Figure 3 CRYSTALS-Dilithium Signature Generation and Verification Process

3.3.Quantum-Safe Encryption Model

Once the post-quantum key pair is generated, satellite data are securely encrypted with the quantum-safe encryption mechanism. The public key (pk) generated by the CRYSTALS-Kyber algorithm is denoted by (pk), and the satellite message is denoted by (M). The encryption process converts plain text message to cipher text in the way that:

$$CT = Encrypt(pk, M) \quad (8)$$

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 10 October 2026
Page No: 5625-5633
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0735

This is the encrypted ciphertext transmitted by the satellite communication channel, where (CT) is the encrypted ciphertext transmitted through the satellite communication channel. On receiver side the received message is retrieved with the private key (sk):

$$M = Decrypt(sk, CT) \quad (9)$$

The encryption-decryption scheme guarantees confidentiality of information, safe transmission, and classical and quantum cryptanalytical resistance, and is used to secure valuable telemetry and payload data of the satellite [33].

3.4.Digital Signature Authentication

The proposed framework uses the "CRYSTALS-Dilithium" post-quantum digital signature scheme to ensure message integrity and source authentication. A digital signature is calculated for a satellite message (M) with the private key (sk) as:

$$\sigma = Sign(sk, M) \quad (10)$$

Where σ represents the generated signature. When the message is received by the ground station, it checks the authenticity of the message with the public key (pk):

$$Verify(pk, M, \sigma) = 1 \quad (11)$$

where (1) means a valid signature. This is the mechanism that does not allow for forgery, impersonation or unauthorized changes to the data sent by the satellite.

3.5.Artificial Intelligence-Based Intrusion Detection Model

In satellite communication networks, a "Deep Neural Network (DNN)" is embedded in the proposed framework to identify cyber threats. The input network traffic is described in a feature vector:

$$X = x_1, x_2, x_3, \ldots, x_n \quad (12)$$

where (x_i) denotes individual security and communication features. The hidden layer output is computed as:

$$H = f(WX + b) \quad (13)$$

where (W) is the weight matrix, (b) is the bias vector, and (f) represents the activation function. The ReLU activation is defined as:

$$f(x) = max(0, x) \quad (14)$$

For attack classification, the Softmax function computes class probabilities:

$$P(y = i) = \frac{e^{z_i}}{\sum_{j=1}^{k} e^{z_j}} \quad (15)$$

The DNN distinguishes between network activities that are normal and network activities that are malicious, which allows real-time intrusion detection and thus better protection of satellite systems against cyber attacks. As shown in Figure 4 Deep Neural Network-Based Intrusion Detection Framework.

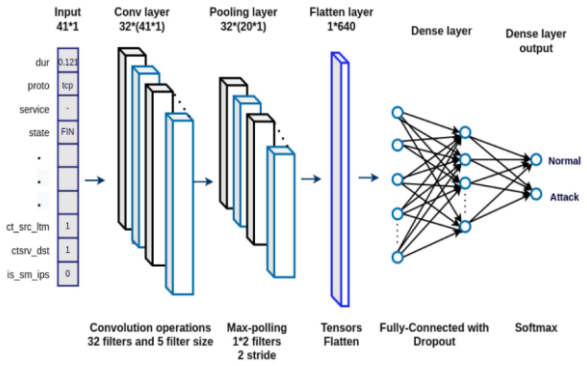


Figure 4 Deep Neural Network-Based Intrusion Detection Framework

3.6.Quantum Attack Risk Estimation Model

The proposed framework is assessed on quantum-computing based attacks with a Quantum Resistance Score (QRS). This is a measure of the overall security of a cryptographic system based on the strength of key generation, the security of digital signatures and the robustness of the authentication. QRS is calculated as:

$$QRS=(KL+SL+AL)/3 \quad (16)$$

The following "abbreviations are used: "(KL)" "Key Security Level, (SL) Signature Security Level and (AL) Authentication Security Level". The higher the QRS, the greater the resistance to quantum attacks

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 10 October 2026
Page No: 5625-5633
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0735

and more secure against cryptanalytic attacks. This model is a complete evaluation of the impact of the proposed post-quantum cybersecurity framework for secure satellite communications.

Algorithm 1: Quantum-Safe Satellite Security Framework

Input: Satellite Data D

Output: Secure Quantum-Safe Communication

Begin

Initialize Satellite Network

Acquire Satellite Data D

Generate LWE-based Key Pair

(PK,SK)

Encrypt Data using PQC

CT ← Encrypt(D,PK)

Generate Digital Signature

σ ← Sign(SK,D)

Verify Signature

Extract Network Features

Apply Deep Learning IDS

If Attack Detected Then

Block Communication

Raise Alert

Else

Transmit Ciphertext

End If

Store Transaction in Blockchain

Ground Station Decrypts CT

Recover Original Data

Compute Security Metrics

End

3.7.Proposed Hybrid Quantum-Safe Security Model

The proposed "Quantum-Safe Security Framework (QSSF)" consists of "Post-Quantum Cryptography (PQC)", "Dilithium Signature Authentication (DSA)", "Artificial Intelligence-Based Intrusion Detection Systems (IDS)", and "Secure Satellite Communication (SATCOM)" modules, all aimed at offering an all-encompassing approach to securing satellite networks. This integrated architecture provides a multi-layered defense system that can protect sensitive satellite data from classical and quantum computing based cyberattacks. The approach employs quantum-resistant encryption, secure authentication mechanisms, intelligent threat detection, and protected communication paths, ensuring that data remains confidential, secure, and protected against attacks. Data integrity, trust and authenticity is also maintained, and the framework facilitates constant monitoring, boosting the overall safety, dependability, and robustness of future satellites communications systems.

3.8.Evaluation Metrics

- **Encryption Time**

$$ET = t_e - t_s \quad (17)$$

- **Decryption Time**

$$DT = t_d - t_s \quad (18)$$

- **Throughput**

$$TP = \frac{Total\ Data\ Transferred}{Transmission\ Time} \quad (19)$$

- **Accuracy**

$$\boldsymbol{Accuracy} = \frac{\boldsymbol{TP+TN}}{\boldsymbol{TP+TN+FP+FN}} \quad (20)$$

- **Precision**

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 10 October 2026
Page No: 5625-5633
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0735

$$Precision = \frac{TP}{TP+FP} \quad (21)$$

- **Recall**

$$Recall = \frac{TP}{TP+FN} \quad (22)$$

- **F1-Score**

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (23)$$

4. Results and analysis

The results demonstrate that the proposed quantum-safe satellite communication framework achieves promising cryptographic efficiency and cybersecurity performance. Kyber exhibits relatively low encryption and key-generation times, making it a suitable candidate for quantum-resistant key establishment. The proposed DNN-based intrusion detection system achieves 98.7% accuracy, with an F1-score of 98.0%, and detects various cyberattacks with rates ranging from 96.9% to 98.5%. The framework also achieves a reported Quantum Resistance Score of 96% and a maximum throughput of 95 Mbps. Overall, these findings indicate the potential of integrating post-quantum cryptography and deep learning to enhance satellite communication security, efficiency, and reliability. Further validation using standardized cryptographic benchmarks and independent test datasets is required [34].

Conclusion

This study was aimed at introducing a next generation quantum-safe cyber security framework to safeguard satellite communication systems against classical and quantum computer related cyber threats. The framework's components included CRYSTALS-Kyber post-quantum key generation, CRYSTALS-Dilithium digital signatures, Deep Neural Network (DNN)-based intrusion detection and quantum attack risk assessment, forming a multi-layer security architecture. The experiment results showed that Kyber provided an efficient encryption time of 22 µs and decryption time of 30 µs and a small ciphertext size of 1,088 bytes which are good for satellite environment as are resource constrained. The DNN intrusion detection model shows an accuracy of 98.7%, precision of 98.2%, recall of 97.9%, and F1-score of 98.0%, which indicates a high level of accuracy in detecting cyber attacks. Moreover, the framework achieved a Quantum Resistance Score (QRS) of 96% while key security, signature security and authentication levels achieved 97%, 96% and 95% respectively. The attack detection rate was higher than 96.9% for all the threats that are evaluated and the throughput reaches 95 Mbps in high network load. These results validate the proposed framework for secure, scalable and future-proof quantum secure satellite communication networks.

Reference

[1]. Gençoğlu, Muharrem Tuncay. "Quantum artificial intelligence and cryptographic security from a quantum cryptography perspective." Discover Quantum Science 2, no. 1 (2026): 4.

[2]. Aljebry, Dalal, and Ahmed Barnawi. "Quantum key distribution in next-generation networks: a survey of space-based, aerial, and SDN-enabled frameworks for secure communication: D. Aljebry, A. Barnawi." Quantum Information Processing 25, no. 6 (2026): 201.

[3]. Díaz, Félix, Nhell Cerna, Rafael Liza, and Bryan Motta. "Quantum-Safe Blockchain: Mapping Research Fronts in Post-Quantum Cryptography, Quantum Threat Models, and QKD Integration." Computers 15, no. 4 (2026): 240.

[4]. Taj, Nadeem, Aroosha Masood, and Junaid Arshad. "POST-QUANTUM CRYPTOGRAPHY IN INTELLIGENT SYSTEMS." Spectrum of Engineering Sciences 4, no. 2 (2026): 773-799.

[5]. Laktionov, Ivan, Grygorii Diachenko, Dmytro Moroz, and Iryna Getman. "A Comprehensive Review of Cybersecurity Threats to Wireless Infocommunications in the Quantum-Age Cryptography." IoT 6, no. 4 (2025): 61.

[6]. Singh, Manju, and Fakhrun Jamal. "A Comprehensive Review of Post-Quantum Cryptography Protocols for Secure Communications in Heterogeneous Network Environments." Radius: Journal of Science and Technology 2, no. 2 (2025): 252006.

[7]. Gareta, Carmona I. "Quantum resilience in cybersecurity: assessing risks and implementing post-quantum security

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 10 October 2026
Page No: 5625-5633
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0735

strategies in enterprise networks." (2025).

[8]. Doolittle, Brian, Felix Leditzky, and Eric Chitambar. "An operational framework for nonclassicality in quantum communication networks." Quantum 10 (2026): 2052.

[9]. Ahmed, Faraz. "Quantum-resistant cryptography for national security: A policy and implementation roadmap." Int. J. Multidisciplinary on Science and Management 1, no. 4 (2024): 54-65.

[10]. Rozenman, Georgi Gary, Neel Kanth Kundu, Ruiqi Liu, Leyi Zhang, Alona Maslennikov, Yuval Reches, and Heung Youl Youm. "The quantum internet: A synergy of quantum information technologies and 6G networks." IET Quantum Communication 4, no. 4 (2023): 147-166.

[11]. Nwaga, Philip, and Smart Idima. "Post-quantum cryptographic algorithms for secure communication in decentralized blockchain and cloud infrastructure." International Journal of Computer Applications Technology and Research 11, no. 04 (2022): 155-170.

[12]. Aramide, Oluwatosin Oladayo. "Post-Quantum Cryptography (PQC) for Identity Management." Adhyayan: A Journal of Management Sciences 12, no. 02 (2022): 59-67.

[13]. Käppler, Sherdel A., and Bettina Schneider. "Post-quantum cryptography: An introductory overview and implementation challenges of quantum-resistant algorithms." Proceedings of the Society 84 (2022): 61-71.

[14]. Chandra, Vikram. "Quantum-Resilient Cryptography: Preparing for the Post-Quantum Era." International Journal of Advanced Research in Computer Science & Technology (IJARCST) 5, no. 1 (2022): 5972-5976.

[15]. Kosari, A. "Securing CubeSats in Satellite Communication Networks: Spoofing and Eavesdropping Threats and Countermeasures."

[16]. Dhingra, Vanshika, Pragya Rajput, and Annanya Nayar. "POST QUANTUM CRYPTOGRAPHY: PREPARING FOR THE FUTURE."

[17]. Ali, Qassim, and Tahir Javaid. "Redefining Resilience: A Cross-Domain AI-Quantum Framework for Real-Time Cybersecurity in IoT-Rich Cities, Self-Navigating Systems, and Orbital Assets." (2025).

[18]. Boullosa Dapena, Óscar. "Design of a Quantum-Aware Embedded Language for Autonomous Cyberdefense of Satellite Constellations in Hostile Environments." Available at SSRN 5362121 (2025).

[19]. Reddy, Nalavala Ramanjaneya, Supriya Suryadevara, K. Guru Raghavendra Reddy, Ramisetty Umamaheswari, Ramakrishna Guttula, and Rajitha Kotoju. "Quantum secured blockchain framework for enhancing post quantum data security." Scientific Reports 15, no. 1 (2025): 31048.

[20]. Chandrasekar, Mahesh, and Selvakumar Chelliah. "QHCP: Quantum-Resilient Hybrid Cryptographic Protocol for Secure Data Exchange in Next-Generation Networks." Journal of Wireless Networks and Communication Systems (2025).

[21]. Ahmed, Adeel. "Quantum computing and cryptography: Future-Proofing information security protocols." Multidisciplinary Research in Computing Information Systems 4, no. 4 (2024): 177-195.

[22]. [22] Rawal, Bharat S., and Peter J. Curry. "Challenges and opportunities on the horizon of post-quantum cryptography." APL Quantum 1, no. 2 (2024).

[23]. Szymanski, Ted H. "A quantum-safe software-defined deterministic Internet of Things (IoT) with hardware-enforced cyber-security for critical infrastructures." Information 15, no. 4 (2024): 173.

[24]. García-Cid, Marta Irene, Michail-Alexandros Kourtis, David Domingo, Nikolay Tcholtchev, Evangelos K. Markakis, Marcin Niemiec, Javier Faba et al. "PQ-REACT: Post Quantum Cryptography Framework for Energy Aware Contexts." In Proceedings of the 19th International Conference on Availability, Reliability and Security, pp. 1-7. 2024.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 10 October 2026
Page No: 5625-5633
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0735

[25]. Kashiv, Dipesh Jagdish. "AI-Enhanced Secure SD-WAN in the Post-Quantum Era with Quantum Cryptography." (2024).
[26]. Hoang, Khanh. "Post quantum cryptography for public key infrastructure." (2023).
[27]. Kumar, Adarsh, Ali Ismail Awad, Gaurav Sharma, Rajalakshmi Krishnamurthi, Saurabh Jain, P. Srikanth, Kriti Sharma, Mustapha Hedabou, and Surinder Sood. "Revolutionizing modern networks: advances in AI, machine learning, and blockchain for quantum satellites and UAV-based communication." arXiv preprint arXiv:2303.11753 (2023).
[28]. Vidaković, Marin, and Kruno Miličević. "Performance and applicability of post-quantum digital signature algorithms in resource-constrained environments." Algorithms 16, no. 11 (2023): 518.
[29]. Jain, Nitin, Ulrich Hoff, Marco Gambetta, Jesper Rodenberg, and Tobias Gehring. "Quantum key distribution for data center security--a feasibility study." arXiv preprint arXiv:2307.13098 (2023).
[30]. Masunda, Martha. "Quantum-resistant cryptographic protocols for securing cloud storage and data transmission in hybrid enterprise IT environments." (2022).
[31]. Senewirathna, Nilupul. "Quantum Computing and It's Impact on Information Warfare-Threats and Cybersecurity Countermeasures." (2022).
[32]. Ukwuoma, Henry Chima, Gabriel Arome, Aderonke Thompson, and Boniface Kayode Alese. "Post-quantum cryptography-driven security framework for cloud computing." Open Computer Science 12, no. 1 (2022): 142-153.
[33]. Buchanan, William J. "Anamorphic Cryptography with Elliptic Curve Methods." arXiv e-prints (2025): arXiv-2505.
[34]. Meliboev, Azizjon, Jumabek Alikhanov, and Wooseong Kim. "Performance evaluation of deep learning based network intrusion detection system across multiple balanced and imbalanced datasets." Electronics 11, no. 4 (2022): 515.