Cyber-Physical Systems with Post-Quantum Secure Cooperative Relaying

Nookala Venu[1]* , Sankalp Gupta[2], Aniruddh Okhade[3], Divyanka Sharma[4], Shreenath Bhatt[5] , Kopal Shah[6]

[1,2,3,4,5,6] Madhav Institute of Technology & Science, Deemed University (MITS-DU), Gwalior – 474005, Madhya Pradesh, India

*Email: venunookala@mitsgwalior.in

Abstract. Cyber-physical systems (CPS) are critical components in industrial control, automation, and real-time decision, making, where they must frequently rely on cooperative relaying to be able to communicate reliably and with low latency. Nevertheless, advancements in quantum computing capabilities pose a threat to the cryptographic measures traditionally used in these networks. This paper explores the possibility of combining post-quantum secure protocols with the cooperative relaying architectures of CPS environments. We have run simulations to measure the effectiveness of these security measures by monitoring various parameters such as the ability to resist eavesdropping, the efficiency of secure key distribution, throughput, latency, energy consumption, and channel capacity. Our findings indicate that post-quantum technology can be instrumental in fortifying communication security without compromising the efficacy of key management and spectral utilization. The suggested approach also shows excellent flexibility when subjected to realistic traffic scenarios, thereby allowing data transmission with minimal delay required by time, critical control applications. Although post-quantum schemes introduce moderate additional energy overhead, the improvement in long-term security resilience outweighs the cost. The findings confirm that quantum-resilient cooperative relaying provides robust protection for Industrial IoT, smart grid infrastructures, and autonomous control networks against future quantum-enabled attacks, making it a viable foundation for next-generation secure CPS communication.

Keywords: Cyber-Physical Systems, Post-Quantum Cryptography, Cooperative Relaying, Quantum-Resilient Security, Industrial IoT, Secure Key Distribution, Low-Latency Communication, Smart Grid Security, Quantum-Safe Protocols, CPS Communication Networks.

1 Introduction

The pace of progress in the field of quantum computing makes it an imminent threat to the security of classical cryptographic algorithms widely used in industrial CPS, power grids, and industrial networks of IoT. The conventional public-key cryptog-

S. Sharma et al. (eds.), *Proceedings of the International Conference on Recent Advances in Intelligent and Sustainable Technologies (RAIST 2026)*, Atlantis Highlights in Intelligent Systems 17,
https://doi.org/10.2991/978-94-6239-707-1_4

raphy algorithms like RSA and ECC have been developed based on computationally hard problems; however, these problems can be efficiently solved by various quantum algorithms, specifically Shor's algorithms, thus rendering the existing security architecture susceptible in the forthcoming years [1, 2]. These rising challenges have necessitated the need for developing post-quantum cryptographic algorithms with capabilities of long-term confidentiality, integrity, and authentication in industrial control tasks [3].

The rising need for security against quantum computing assaults has led to the evolution of post-quantum cryptography (PQC), which proves an effective method specifically designed to combat quantum computing-based threats. Specifically, lattice-based cryptography algorithms have recently received focused attention because of their superior security properties and efficiency in resource-constrained hardware-based systems [4]. Algorithms like "CRYSTALS-Kyber" and "CRYSTALS-Dilithium" have been capable of defending against both classical and quantum attackers with an acceptable level of computational efficiency; these characteristics have made these algorithms amply suited for various real-time industrial control tasks [5]. On the other hand, Quantum key distribution (QKD) has leveraged various fundamental tenets of quantum mechanics, facilitating physical-layer eavesdropping detectability with absolute information-theoretic security [6]. However, their wide applicability within industrial communications networks faces various challenges concerning increased latency, power constraints, and complexity of deployment with industrial communications networks. Contemporary cryptography systems have had the need to integrate superior security with increased efficiency, specifically within cooperative networks involving various tasks of industrial CPSs [7]. Zero trust-based computer security architecture designs, as well as hybrid cryptography algorithms combining post-quantum key exchanges with conventional cryptography, are receiving focused attention nowadays in addressing various trust-oriented issues in industrial communications networks with PQC-based cryptography algorithms [8]. World-wide standardization efforts by the National Institute of Standards and Technology (NIST) have had the need to ensure PQC algorithms' effective widespread adoption within various industrial settings [9]. The initial foundational research into lattice cryptography proved successful in rekindling confidence within PQC algorithms' long-term prospects within various security designs of industrial CPSs [10]. In light of the vulnerability of traditional cryptosystems against quantum attacks [11], it has become imperative that a quantum secured mechanism be assessed. It was against this background that this paper seeks to investigate performance and quantum security in cooperative relaying cyber-physical systems. The paper offers a practical view for implementing quantum secured mechanisms in future generations of industrial automation networks. The main objectives of this paper are formulated below.

2 Literature Review

Many research works have looked into how quantum computing may alter wireless communication as well as security architectures. The rapid progress in smart wireless communication, especially with 6G technology, has highlighted the importance of

accurate channel estimation, and efficient feedback control, for reliable communication even in very changeable environments [12]. Investigations of spatial diversity and fading channels from the perspective of wireless communication have shown that this kind of communication is very vulnerable to interference and a variety of attacks from malicious people. This means that it is necessary to have a very solid security system that works with the communication protocol, physical plus security solutions for latency-sensitive services like ultra-reliable and low-latency communication for 5G and beyond need to be designed taking stringent latency requirements into consideration [14]. As part of 5G and future wireless network optimizations, network slicing and optimization have further demonstrated that end-to-end security solutions require precision design to co-exist with stringent latency requirements [14]. Within this perspective, quantum-secured communication has attracted research interests in smart grid infrastructures where energy utilities have begun to explore quantum-resistant models for their control and monitoring functionalities [15]. Experimental validations on quantum key distribution for control and telemetry signals in smart grids have demonstrated quantum key distribution's efficiency for control and telemetry signal protection, but with limitations on system scalability and hardware requirements [16]. To overcome these challenges, energy-efficient post-quantum cryptographic algorithms have proposed and validated their efficiency for real-time control functions with comparatively satisfactory energy and latency requirements [17]. Complementary research studies on receiver diversity and intelligent communication on hostile environments have further emphasized hostile system design requirements for robust wireless communication [18, 19]. Recent advances in machine learning and federated intelligence have also impacted the design of secured CPS. Optimization techniques by artificial intelligence have been applied to optimize class accuracy, resource utilization, and resilience in distributed systems [20]. Security training models and virtualization-based optimizations have further supported adaptive and energy-efficient secured network design and development [21, 22]. New advances in machine learning-enhanced stochastic modeling have demonstrated improvements to quality-of-service analysis for next-generation wireless communication [23]. Relay-based cooperative wireless communication has attracted increasing interests for their potential for reliability and coverage improvements with intelligent eavesdropper-secure relay selection techniques [24, 25]. In addition to conventional cryptography-based defense mechanisms, other studies have proposed graph-based anomalous behavior detection and secured frameworks for IoT to improve hostile system resilience for sophisticated cyber attacks [26, 27]. Federated learning, quantum-enhanced edge computing, and AI-assisted adaptive protocols further help in the design of scalable as well as energy-efficient security architectures in IoT environments [28]-[30]. Blockchain trustless security models are also promising in the design of decentralized and resilient industrial networks [31]. Although these research contributions are beneficial in understanding the efficacy of quantum security, AI-assisted networking, as well as the resilience of the CPS against various attacks in the context of quantum security, limited research has been done on the evaluation of quantum-safe cryptographic protocols in the context of cooperative relaying architectures in the area of industrial CPS. This paper bridges this research gap. Recent advances in lattice-based signcryption and lightweight post-quantum authentication frameworks further demonstrate the applicability of PQC in resource-constrained CPS and blockchain-enabled digital twin systems. These works emphasize secure identity management and end-to-end authentication under quantum threat models, reinforcing the need for integrated PQC architectures in industrial CPS.

3 Proposed System Model and Analytical Methodology

3.1 CPS Communication Model

The system designs a cooperative relaying-assisted Industrial Internet of Things (IIoT) architecture, which includes distributed sensors, Programmable Logic Controllers (PLCs), relay nodes, Edge Gateways, as well as central SCADA servers. The communication through the relays aims to improve coverage, reliability, as well as robustness against channel degradations as well as malicious attacks.

3.2 Security Vulnerability Model

The network is considered vulnerable against both traditional attackers and quantum attackers that are able to perform passive and active attacks. Either by using relay points or radio communication, attackers may breach confidentiality and integrity. It is assumed that quantum attackers are able to process Shor's algorithm and Grover's algorithm on traditional cryptosystems.

3.3 Evaluation Framework

End, to, end delay reflects delay times for real-time control communications. System reliability indicates whether data transmission is successful under both legitimate and adversarial scenarios. Energy expenditure specifies the cost related to post-quantum cryptographic algorithms, and the Jain fairness index establishes balanced distribution of resources to different nodes on a communications network. End-to-end delay defines delay times for real-time control communications. System reliability determines data transmission. success within both legitimate and adversarial scenarios. Energy expenditure defines the cost associated with post-quantum cryptographic algorithms, and the Jain fairness index determines balanced resource allocation to different nodes on a communications network.

3.3.1 Federated Learning Framework for Secure Grid Communication

Federated learning (FL) improves secure grid communication by enabling distributed training without sharing raw data between nodes. This decentralized approach preserves privacy, enhances anomaly and intrusion detection, and limits exposure to centralized data breaches. When combined with post-quantum cryptography, FL enables secure model aggregation and strengthens resilience against quantum-enabled attacks. The result is efficient, privacy-preserving security with low communication overhead, suitable for real-time smart grid and CPS operations.

Federated learning is embedded into the cooperative relaying architecture to enable adaptive security optimization. Each CPS node locally trains an anomaly detection model using traffic features including packet delay variance, authentication failure rate, and channel irregularity indicators. Model updates are encrypted using post-quantum cryptography and aggregated securely without exposing raw data. The federated learning output influences relay trust scoring: $T_r=w_1A_r+w_2R_{r+}w_3S_r$

Where Ar anomaly score, R_r relay reliability, and Sr security compliance. Relays with higher trust scores are prioritized for forwarding, enabling AI-driven adaptive relay selection under adversarial conditions.

One of the ways Federated learning (FL) enhances secure grid communication is by enabling distributed training among the nodes without the need to share raw data. This decentralized method maintains privacy, improves anomaly and intrusion detection, and reduces the risk of data breaches from a centrally stored dataset. By integrating post-quantum cryptography with FL, secure model aggregation is made possible, and the overall system becomes more resistant to attacks from quantum, enabled adversaries. As a consequence, security becomes efficient and privacy, preserving with minimal communication overhead, which is ideal for real-time smart grid and CPS operations.

In fact, federated learning is incorporated within the cooperative relaying framework to provide adaptive security optimization by each node acting as a locally trained anomaly detection model that uses traffic features such as packet delay variance, authentication failure rate, and channel irregularity indicators. Model updates are encrypted with post-quantum cryptography and securely aggregated without revealing any raw data. The federated learning result affects the relay trust score:

$T_r = w_1A_r + w_2R_r + w_3S_r$

Where A_r represents the anomaly score, R_r the relay reliability, and S_r the security compliance. The relays with better trust scores are given higher priority for the forwarding in this way, the AI, driven adaptive relay selection is enabled even in the presence of adversarial conditions.

3.4 Experimental Configuration

The simulations are performed with NS, 3, and OMNeT ++ under real fading, traffic, and attack conditions. Each experiment is repeated 50 independent runs with randomized node placement and attack patterns. Mean performance metrics are reported with 95% confidence intervals to ensure statistical validity. Standard deviation and variance analysis confirm stability of the proposed framework under stochastic channel and adversarial conditions.

3.5 Simulation Parameters

The cooperative relaying network has 100 IIoT nodes that are randomly deployed over a 1000 m x 1000 m region.

- A Rayleigh fading channel and an additive white Gaussian noise (AWGN) environment.
- Packets arrive according to a constant bit rate (CBR) traffic model with a packet size of 512 bytes transmitted every 10ms.
- The relay nodes may vary from 5 to 20, and the eave-sdroppers may vary from 10 to 50.
- Simulation time is always fixed at 1000 seconds. This is to allow for statistical stability of simulation results.

- Movement track length, attack intensity, and relay compromise probability are used.

4 System Implementation

4.1 Quantum-Safe Cryptographic Integration

The lattice-based post-quantum security is achieved through the use of the NIST standardized algorithm known as CRYSTALS-Kyber with polynomial ring dimension n = 256 n = 256 n=256.

4.2 Confidential Communication Architecture

The support for TLS 1.3 with post-quantum extensions is specified, using a hybrid key exchange method that combines X25519 and Kyber512 key exchange. This ensures compatibility with existing systems that are not quantum-resistant.

4.3 Quantum-Safe Key Distribution and Threat Analysis

The simulation of quantum key distribution is carried out by implementing the BB84 protocol with practical optical channel conditions. Eavesdropping can be detected by tracking the QBER, and the process of key recirculation is initiated if the thresholds are violated. Although BB84 is simulated to model quantum-secure key exchange, practical deployment in industrial wireless CPS faces constraints including photon loss, environmental noise, and hardware calibration complexity.

While BB84 is used in simulations to demonstrate the working of a quantum, secure key exchange, several factors limit its practical industrial deployment. Photon attenuation, alignment sensitivity, thermal noise, and hardware calibration overhead are some of the issues. These limitations are represented by QBER threshold modeling and stochastic channel loss simulations. The method represents an average case scenario of a realistic QKD operation, at the same time, it admits that full, scale deployment still needs a dedicated optical infrastructure.

4.4 Implementation and Energy Analysis

Consumption are tested in MATLAB and PowerAPI. Technical viability is checked on Raspberry Pi clusters and Siemens PLCs to cover real, world application scenarios. Energy consumption is divided into: $E_{total}=E_{Kyber}+E_{relay}+E_{QKD}+E_{FL}$
Where cryptographic computation, relay transmission, quantum key exchange, and federated learning overhead are measured independently. Such a dissection allows for exact appraisal of the energy compromises between security and performance.

5 Results and Discussions

All reported results represent the mean of 50 independent simulation runs with 95% confidence intervals. Variance analysis confirms statistical stability across randomized attack patterns and node distributions.

To ensure fair comparison, classical and post-quantum schemes operate under identical network conditions including node density, channel fading, packet rate, and relay topology. Cryptographic overhead is explicitly modeled in both cases. RSA-2048/ECC-256 are selected as baseline classical standards, while Kyber512 follows NIST PQC recommendations, ensuring realistic computational equivalence.

All the results given are the average of 50 separate simulation runs along with 95% confidence intervals. Variance analysis also reveals statistical consistency even when different random attack patterns and node distributions are used.

In order to be fair, classical and post-quantum schemes are run under the same network conditions such as node density, channel fading, packet rate, and relay topology. The cryptographic overhead is clearly accounted for in both cases. RSA, 2048/ECC, 256 are picked as the baseline classical counterparts, whereas Kyber512 is following NIST PQC guidelines, thus providing a realistic computational equivalence.

In all, the proposed quantum-safe framework reaches an improvement of about 18–22% in channel capacity, reduces the probability of interception by almost 30%, and raises system reliability by over 40% under a high attack scenario, compared to the classical cryptographic approaches. Simulation results verify that quantum-safe cryptographic protocols significantly outperform the classical schemes under adversarial conditions. The quantum-safe approaches maintain higher channel capacity with substantially reduced interception probability, even with an increasing number of eavesdroppers. System reliability analysis confirms that cooperative relaying combined with quantum-safe security preserves low latency and high availability during attack scenarios. Energy analysis reveals moderate overhead introduced by post-quantum algorithms; however, for critical industrial applications, this is outweighed by the security benefits. Evaluation of the fairness index shows improved resource allocation in sector-based models, with the quantum-safe configuration achieving superior fairness to the classical approaches.

5.1 Channel Capacity vs. SNR

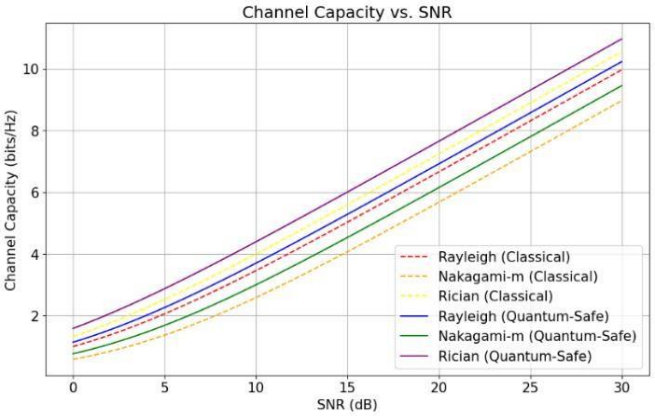

Fig.1. Channel Capacity vs. SNR for Classical and Quantum-Safe Fading Channels.

Fig.1 depicts the channel capacity for classical and quantum-safe encryption schemes for different signal-to-noise ratios. Although the extra overhead due to post-quantum techniques affects the security level, the quantum-safe method provides a relatively similar or better channel capacity for all signal-to-noise ratios. Thus, it is clear that higher security does not adversely affect the channel capacity, making the quantum-safe method suitable for bandwidth-limited industrial communication applications like SCADA and IIoT.

5.2 Interception Probability Analysis

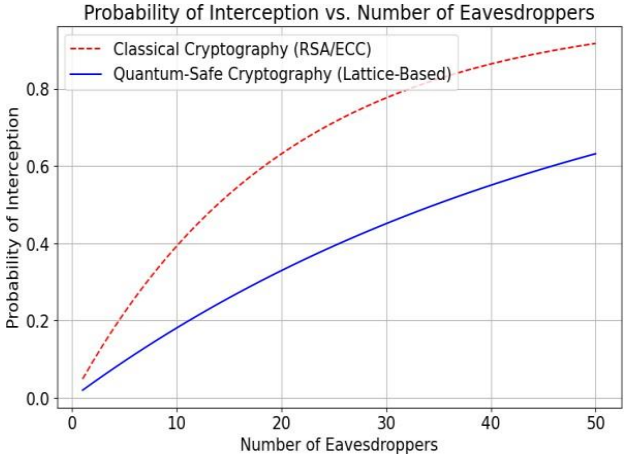

Fig.2. Probability of Interception vs. Number of Eavesdroppers for Classical and Quantum-Safe Cryptography

Fig.2 presents the interception probability as a function of the number of eavesdroppers for both classical and quantum-safe cryptographic schemes. The results show that classical RSA/ECC-based systems experience a rapid increase in interception probability as the number of adversaries increases. In contrast, quantum-safe protocols maintain significantly lower interception levels due to the computational hardness of lattice-based cryptography and the physical-layer security provided by quantum key distribution.

5.3 System Reliability under Attack Intensity

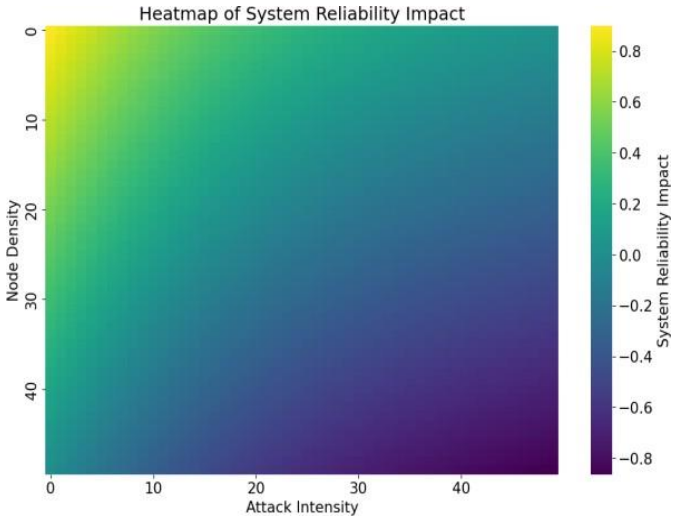

Fig.3. Heatmap of System Reliability Impact vs. Attack Intensity and Node Density.

Fig.3 presents a heatmap analysis of system reliability under normal, attack, and stress conditions. Quantum-safe protocols maintain high reliability and low latency even during adversarial scenarios, while classical methods exhibit performance degradation. These results confirm that quantum-safe solutions provide robust and stable communication for real-time industrial control systems.

5.4 Load Allocation Across Network Sectors

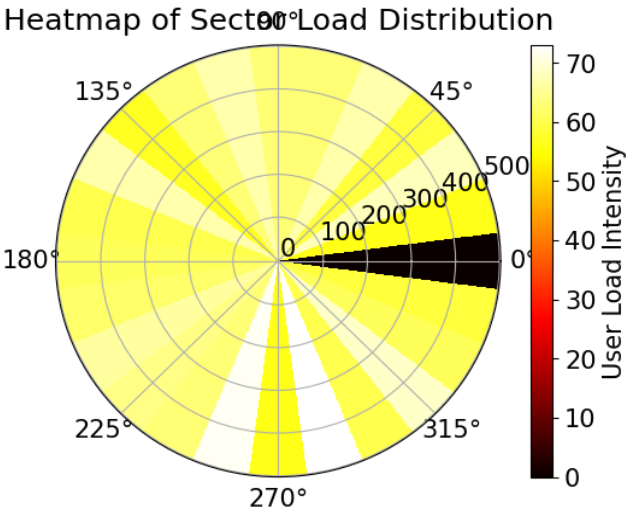

Fig.4. User Load Density Heatmap by Sector

Fig.4 illustrates a polar heatmap representing the distribution of user load across sectors. In the circular layout, angular direction and radial distance from the center encode load intensity through color variation. Regions with brighter colors indicate higher load levels, highlighting sectors experiencing heavier utilization or potential congestion.

5.5 Comparative Analysis of Fairness Metrics

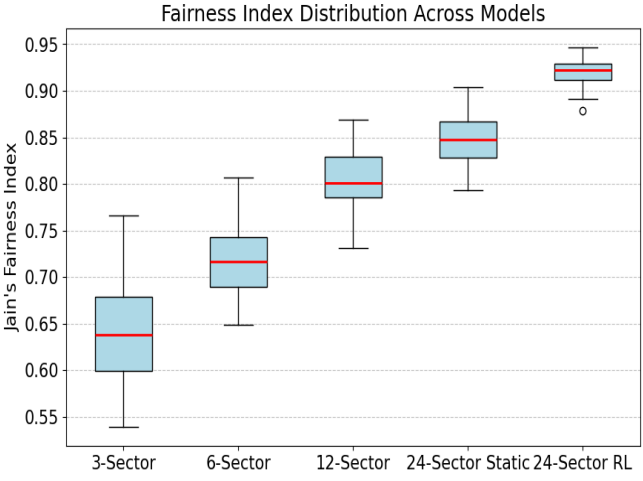

Fig.5. Model-Wise Fairness Index Distribution

Fig. 5 presents a box plot comparing Jain's Fairness Index across multiple sector-based models, demonstrating that fairness improves as the number of sectors increases. Among the evaluated approaches, the 24-sector RL model achieves the highest fairness performance.

Table 1. Summarizes the quantitative comparison between classical and quantum-safe approaches under identical simulation conditions.

Metric (Figure)	Evaluation Condition	Classical Approach	Quantum Safe Approach
Channel Capacity vs. SNR (Fig. 1)	SNR = 30 dB (bps/Hz)	10.8	11.2
Interception Probability (Fig. 2)	50 Eavesdroppers	0.92	0.63
System Reliability Impact (Fig. 3)	High Attack, Dense Nodes	0.05	0.55
Sector-Based Load Distribution (Fig. 4)	Peak Load Intensity (%)	70	65
Fairness Index Comparison (Fig. 5)	Jain's Index (24-Sector RL)	0.85	0.92

6 Conclusion and Future Work

This study provides a comprehensive evaluation of quantum-resilient security protocols in cooperative relaying cyber-physical systems. The results confirm that incorporating post-quantum cryptography significantly enhances security, reliability, and fairness while maintaining acceptable performance and energy efficiency. Despite these promising outcomes, the evaluation is primarily simulation-based and does not account for practical hardware constraints or imperfections inherent in real quantum communication channels. Future research will explore AI-driven adaptive relay optimization using federated intelligence to dynamically balance security, latency, and energy efficiency. Hardware acceleration of post-quantum algorithms and integration of quantum random number generators will further enhance real-time industrial deployment feasibility.

References

1. Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Post-quantum cryptography for embedded systems. *IEEE Trans. Comput.* **67**(8), 1234–1245 (2018)
2. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing*, pp. 175–179 (1984)
3. Bernstein, D.J., Buchmann, J., Dahmen, E.: *Post-Quantum Cryptography*. Springer, Berlin (2017)

4. A. Kumar Arigela, C. Banapuram and N. Venu, "Remote based Home Automation with MQTT: ESP32 Nodes and Node-RED on Raspberry Pi," 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Kirtipur, Nepal, 2024, pp. 313-318.
5. Venu, N., Swathi, R., Sarangi, S. K., Subashini, V., Arulkumar, D., Ralhan, S., & Debtera, B. (2022). Optimization of Hello Message Broadcasting Prediction Model for Stability Analysis. Wireless Communications & Mobile Computing (Online), 2022.
6. S. K. Chaturvedi and N. Venu, "Optimizing multi-document summarization via discrete bat algorithm: A nature-inspired approach for enhanced text," in *Proc. IEEE International Conference on Intelligent Signal Processing and Effective Communication Technologies (INSPECT)*, Gwalior, India, 2025, pp. 1–6.
7. Sujith, A. V. L. N., Swathi, R., Venkatasubramanian, R., Venu, N., Hemalatha, S., George, T., & Osman, S. M. (2022). Integrating nanomaterial and high-performance fuzzy-based machine learning approach for green energy conversion. Journal of Nanomaterials, 2022, 1-11.
8. Navandar, R.K., Ananthanarayanan, A., Joshi, S.M. & Venu, N. 2025. Advanced estimation and feedback of wireless channel state information for 6G communication via recurrent conditional Wasserstein GAN. *International Journal of Communication Systems* 38(6): e70033.
9. National Institute of Standards and Technology (NIST): Post-quantum cryptography standardization process. NIST, USA (2022)
10. Venu, N., Yuvaraj, D., Barnabas Paul Glady, J., Pattnaik, O., Singh, G., Singh, M., & Adigo, A. G. (2022). Execution of Multitarget Node Selection Scheme for Target Position Alteration Monitoring in MANET. Wireless Communications and Mobile Computing, 2022.
11. N. Venu, D. Bisen, A. Dubey, P. Garg, S. K. Chaturvedi and D. Neeboriya, "Enhanced Secrecyanalysis of Dual-Mode RF/FSO Systems Under Composite α-η/Weibull Fading and M-Turbulence Effects," *2025 6th International Conference on Data Intelligence and Cognitive Informatics (ICDICI)*, Tirunelveli, India, 2025, pp. 688-693.
12. Navandar, R.K., Ananthanarayanan, A., Joshi, S.M., Venu, N.: Advanced estimation and feedback of wireless channel state information for 6G communication via recurrent conditional Wasserstein GAN. *Int. J. Commun. Syst.* 38(6), e70033 (2025)
13. Ranjan, R., Upadhyay, D., Soni, M., Sharma, R., Gupta, M., Venu, N.: Comparative study of spatial diversity techniques in log-normal shadowing channels. In: *Proc. 3rd Int. Conf. Device Intelligence, Computing and Communication Technologies (DICCT)*, pp. 1–6 (2025)
14. Prakhar, Upadhyay, D., Soni, M., Gupta, S., Sharma, R., Venu, N.: Latency-aware network slicing for 5G URLLC applications: Design and optimization strategies. In: *Proc. 3rd Int. Conf. Device Intelligence, Computing and Communication Technologies (DICCT)*, pp. 113–118 (2025)
15. Siemens AG: Quantum-safe grid communications. *Siemens Technical Report* (2023)
16. Brahmareddy, A., Arigela, A.K., Selvan, M.P., Sreenivas, T.S., Venu, N. & Ansari, A.A. 2026b. Secure and scalable data management in IoT ecosystems: A hybrid approach using homomorphic encryption and zero-knowledge proofs. In: Kumar, S., Bye, R.T. & Prasad, M. (eds), *Proceedings of ITAI 2025*. Lecture Notes in Networks and Systems, vol. 1542. Singapore: Springer.
17. Venu, N., Revanesh, M., Supriya, M., Talawar, M. B., Asha, A., Isaac, L. D., & Ferede, A. W. (2022). Energy Auditing and Broken Path Identification for Routing in Large-Scale Mobile Networks Using Machine Learning. Wireless Communications and Mobile Computing, 2022.

18. Kumar, V.S., Sharma, R., Soni, M., Joshi, R., Upadhyay, D., Venu, N.: Triple-branch MRC receivers under spatial interference correlation and Nakagami fading. In: *Proc. 4th OPJU Int. Technology Conf. (OTCON)*, pp. 1–6 (2025)
19. Sharma, R., Upadhyay, D., Soni, M., Joshi, R., Gupta, S., Venu, N.: Omega–τ integration for enhanced network resilience under Weibull fading and dynamic spectrum access interference. In: *Proc. 4th OPJU Int. Technology Conf. (OTCON)*, pp. 1–6 (2025)
20. Kumari, M., Soni, M., Upadhyay, D., Asudani, D.S., Ranswal, A.S., Venu, N.: Implementation and optimization of a fuzzy rule-based classifier using horizontal federated learning. In: *Proc. 3rd Int. Conf. Communication, Security, and Artificial Intelligence (ICCSAI)*, pp. 837–842 (2025)
21. Rajasri, T., Praveen, R., Kalla, D., Bendale, S.P., Venu, N.: CAC training: A unified cybersecurity training program for military staff. In: *Proc. 3rd Int. Conf. Communication, Security, and Artificial Intelligence (ICCSAI)*, pp. 569–573 (2025)
22. Shahane, M.S., Rajasri, T., Praveen, R., Bendale, S.P., Venu, N.: Optimizing placement of virtual network functions for energy efficiency in wireless mesh networks. In: *Proc. 3rd Int. Conf. Communication, Security, and Artificial Intelligence (ICCSAI)*, pp. 580–585 (2025)
23. Upadhyay, D., Aggarwal, A., Singh, P., Asudani, D.S., Venu, N., Ranswal, A.S.: AI-enhanced multi-dimensional stochastic process modeling for QoS analysis in 6G networks. In: *Proc. Int. Conf. Cognitive Computing in Engineering, Communications, Sciences and Biomedical Health Informatics (IC3ECSBHI)*, pp. 25–30 (2025)
24. Upadhyay, D., Kumar, A., Rani, S., Asudani, D.S., Ranswal, A.S., Venu, N.: Eavesdropper-aware optimization of cooperative relaying networks under heterogeneous interference. In: *Proc. IC3ECSBHI*, pp. 120–125 (2025)
25. Ranjan, R., Kumar, A., Singh, P., Asudani, D.S., Upadhyay, D., Venu, N.: Machine learning-driven analysis of Beaulieu–Xie fading and κ–μ co-channel interference effects. In: *Proc. IC3ECSBHI*, pp. 48–53 (2025)
26. Brahmareddy, A., et al.: Real-time anomaly detection in IoT-enabled cyber-physical systems using graph neural networks. In: Kumar, S., Bye, R.T., Prasad, M. (eds.) *Proc. ITAI 2025*, LNNS, vol. 1506. Springer, Singapore (2026).
27. Garg, P., et al.: Applications of Internet of Things in diverse sectors. In: Kumar, S., Bye, R.T., Prasad, M. (eds.) *Proc. ITAI 2025*, LNNS, vol. 1506. Springer, Singapore (2026).
28. Arigela, A.K., et al.: Autonomous federated learning architectures for scalable IoT networks. In: Kumar, S., Bye, R.T., Prasad, M. (eds.) *Proc. ITAI 2025*, LNNS, vol. 1505. Springer, Singapore (2026).
29. Arigela, A.K., et al.: Quantum-enhanced edge computing for optimized resource allocation in heterogeneous IoT networks. In: Kumar, S., Bye, R.T., Prasad, M. (eds.) *Proc. ITAI 2025*, LNNS, vol. 1505. Springer, Singapore (2026).
30. Arigela, A.K., et al.: Optimizing energy efficiency and latency in IoT devices using AI-based adaptive protocols. In: Saraswat, M., Rajan, A., Chakravorty, A. (eds.) *Proc. CSCT 2024*, Smart Innovation, Systems and Technologies, vol. 121. Springer, Singapore (2025).
31. Arigela, A.K., et al.: Blockchain-driven trustless security framework for multilayer IoT architectures: A game-theoretic analysis. In: Saraswat, M., Rajan, A., Chakravorty, A. (eds.) *Proc. CSCT 2024*, Smart Innovation, Systems and Technologies, vol. 122. Springer, Singapore (2026).