International Journal of
Technology and
Systems
(IJTS)

A Quantum-Resilient Decentralized Swarm Intelligence Framework for Secure Real-Time Synchronization in Industrial Metaverse Environments

Journal of Technology and Systems

ISSN: 2788-6344 (Online)

Vol. 8, Issue No. 2, pp 61 – 82, 2026 www.carijournals.org

A Quantum-Resilient Decentralized Swarm Intelligence Framework for Secure Real-Time Synchronization in Industrial Metaverse Environments

Dr. Abdinasir Ismael Hashi[1*], Mr. Osman Abdullahi Jama[2], Mr. Abdirizak Mohamed Hashi[3]

[1,2]Somali National University

[3]Jazeera University

https://orcid.org/0009-0009-0635-2609

Accepted: 27th May, 2026, Received in Revised Form: 20th June, 2026, Published: 30th June, 2026

Abstract

Purpose: A secure, low-latency, and scalable synchronization framework is required for the Industrial Metaverse to connect distributed Industrial IoT (IIoT) devices, digital twins, and edge nodes. To accomplish this goal, the study introduces the Quantum-Resilient Decentralized Swarm Intelligence Framework (QR-DSIF) that fuses Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), system-wide trust management via Blockchain technology, Edge Computing architectures, and CRYSTALS-Kyber Post-Quantum Cryptography into one framework.

Methodology: The efficiency of QR-DSIF was shown in the simulation results using Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), Blockchain technology, Edge Computing architectures, and CRYSTALS-Kyber Post-Quantum Cryptography.

Findings: The ACO routing mechanism provided routes that were approximately 650 units in length prior to using this mechanism and had achieved only 22 units after 11 iterations for a routing efficiency of 98%. Trust scores assigned to the blockchain were found to range from 0.64 to 0.98, with an average trust score of 0.85, and the levels of agreement among consensus participants ranged between 85% and 90%. Both encryption and decryption operations consistently maintained their processing time at/under 0.001 ms., while remaining consistent (0.03–0.04 ms.) when using Kyber encryption. PSO convergence produced improvements in fitness of 76.1 to 74.38, while the edge-node loads were balanced within a range of 535 to 620 units. Additionally, synchronization delay was improved from 86 to 75 ms, or approximately 12.8%.

Unique Contribution to Theory, Policy and Practice: These results indicate that QR-DSIF would provide efficient routing, strong security, balanced resource utilization, and reliable synchronization for Industrial Metaverse environments.

Keywords: *Industrial Metaverse, Swarm Intelligence, Post-Quantum Cryptography, CRYSTALS-Kyber, Blockchain Trust Management, Real-Time Synchronization*

Journal of Technology and Systems
ISSN: 2788-6344 (Online)
Vol. 8, Issue No. 2, pp 61 – 82, 2026 www.carijournals.org

1. Introduction

The rapid evolution of industrial digitalization has led to the emergence of the Industrial Metaverse, a virtual–physical integrated ecosystem that combines industrial automation, Internet of Things (IoT), cyber-physical systems, digital twins, edge computing, and immersive technologies such as augmented reality (AR) and virtual reality (VR) [1]. In industrial metaverse environments, machines, robots, sensors, operators, and virtual agents continuously interact in real time to optimize production, monitoring, predictive maintenance, and collaborative manufacturing [2]. However, achieving secure and synchronized communication among distributed industrial entities remains one of the major challenges due to the enormous volume of data exchange, low-latency requirements, and increasing cyber threats [3]. Traditional centralized synchronization frameworks are often vulnerable to single-point failures, data tampering, scalability limitations, and high computational overhead, making them unsuitable for next-generation industrial metaverse infrastructures [4].

Simultaneously, the advancement of quantum computing introduces a serious threat to conventional cryptographic mechanisms used in industrial communication systems [5]. The classical encryption algorithms like RSA and ECC would be vulnerable to quantum attacks because of quantum algorithms like Shor's algorithm that can break the existing public key cryptographic algorithm within reasonable computational time [6]. The implementations of quantum computers would have a significant impact on industrial metaverse platforms, particularly with regard to secure authentication, distributed synchronization and trusted data sharing, highlighting the need for quantum-resilient security architectures [7]. Thus, combining post quantum cryptography with the decentralized intelligence mechanisms is an interesting research area for the security of future computational risks in the industrial cyber physical ecosystems [8].

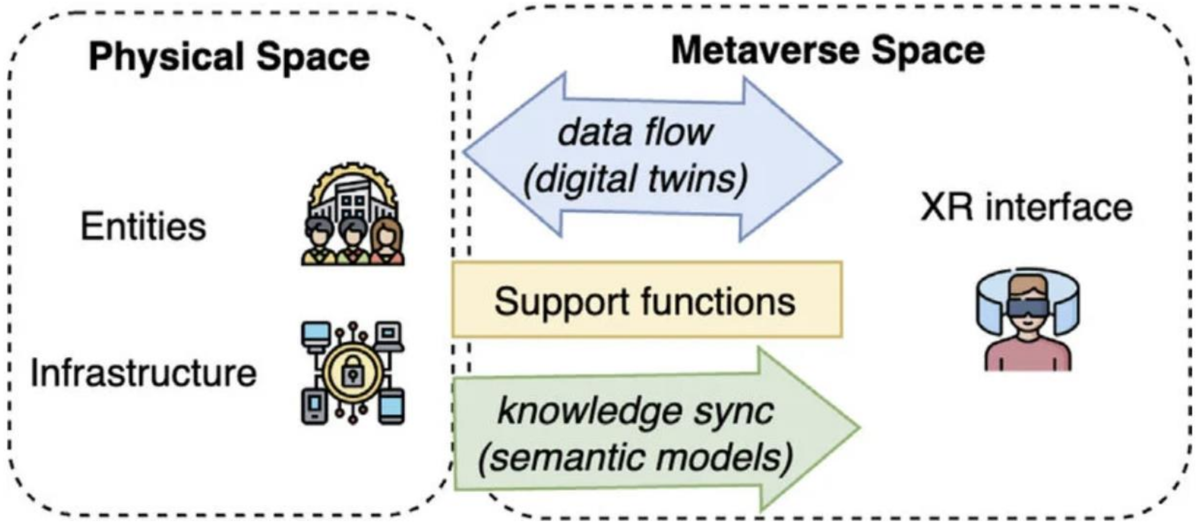

Figure 1: Overview of the proposed industrial metaverse architecture [9].

Collective behavior of biological organisms like ants, bees, birds, and fish schools has drawn great interest as a decentralized computational paradigm named swarm intelligence [10]. Swarm-based systems have characteristics such as self-organization, adaptability, robustness, fault tolerance, and distributed decision making, which are desirable for the dynamic industrial metaverse environment [11]. Swarm intelligence can enhance the scalability, resilience and real-time coordination of distributed industrial networks by allowing autonomous agents to work together to complete synchronization and optimization tasks without needing central controllers [12]. For industrial metaverse architectures, various optimization techniques like Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), and Artificial Bee Colony (ABC) algorithms can be used to optimize synchronization latency, resource allocation, trust management, and secure routing [13].

To overcome these difficulties, the proposed work is designed to integrate these four elements such as decentralized swarm intelligence, blockchain based trust management, edge computing, and post-quantum cryptographic security into an on-going system [14]. According to this architecture, industrial nodes are intelligent swarm agents that can share the synchronization information collaboratively and adapt dynamically to network conditions and cyber threats [15]. In industrial communications, blockchain or distributed ledger technologies offer ways for transactions to be validated immutably and consensus to be reached in a decentralized manner, which helps to ensure transparency and resistance to tampering [16]. At the same time, the sensitive information of industry can be secured from quantum attacks with the help of post-quantum cryptographic algorithms like lattice-based or hash-based encryption algorithms.

Moreover, the framework integrates edge computing to minimize latency and enable real-time processing at the edge, close to the industrial devices [17]. Unlike the conventional centralized approach, the decentralized approach of edge-enabled swarm agents can make the synchronization decisions without relying heavily on remote cloud servers, and reduce the communication delays and enhance the operational efficiency [18]. In industrial metaverse applications like smart manufacturing, robotic coordination, autonomous logistics, remote maintenance, and digital twin interaction, the need for real-time synchronization is especially paramount, as minor delays or synchronization errors can result in production downtimes, operational instability, or safety risks [19]. The proposed framework is based on the concept of swarm intelligence and decentralized coordination at the edge, which improves the accuracy, reliability and scalability of synchronization in a large-scale industrial ecosystem.

In this paper, a Quantum-Resilient Decentralized Swarm Intelligence Framework (QR-DSIF) is proposed for real-time synchronization in Industrial Metaverse environments to achieve security. The proposed framework combines the functionalities of the swarm intelligence algorithms, trust management and blockchain technologies, edge computing, Industrial Internet of Things (IIoT), digital twin, and post-quantum cryptography to enable secure, scalable and low-latency communication in the industrial sector. The following are the research objective of the study:

Journal of Technology and Systems
ISSN: 2788-6344 (Online)
Vol. 8, Issue No. 2, pp 61 – 82, 2026 www.carijournals.org

- To design a quantum-resilient decentralized swarm intelligence framework for secure real-time synchronization in Industrial Metaverse environments.
- To integrate swarm intelligence algorithms such as PSO and ACO for adaptive coordination and synchronization optimization among industrial nodes.
- To incorporate post-quantum cryptographic techniques, particularly the CRYSTALS-Kyber model, to protect industrial communication against future quantum computing attacks.
- To reduce synchronization delay, communication latency, and computational overhead using edge computing and decentralized processing mechanisms.
- To evaluate the proposed framework using MATLAB and Python simulations based on performance metrics such as throughput, packet delivery ratio, scalability, energy consumption, and security resilience.

2. Research methodology

2.1 Proposed Framework Design

The proposed Quantum-Resilient Decentralized Swarm Intelligence Framework (QR-DSIF) aims at offering secure, scalability, and real-time synchronization for Industrial Metaverse environments. It incorporates various concepts such as decentralized swarm intelligence, blockchain-based trust management, edge computing, Industrial Internet of Things (IIoT), digital twins, and post-quantum cryptography in a coherent design. In Industrial Metaverse systems, thousands of sensors, robots, autonomous machines and virtual digital twins are constantly sharing real-time data with each other. Centralized synchronization methods add latency, bottlenecks and single point security failures. The proposed framework overcomes these drawbacks by introducing decentralized swarm agents that self-organize synchronization tasks based on principles from collective intelligence, which are modeled after ant colonies and particle swarms. Each industrial node is an intelligent swarm agent that can be integrated to make decisions locally, verify trust and adaptively synchronize. It is composed of five layers: perception layer, edge intelligence layer, swarm coordination layer, blockchain security layer and Industrial Metaverse application layer.

At the perception layer, IIoT devices continuously generate industrial operational data represented as:

$$S(t) = \{s_1(t), s_2(t), s_3(t), \dots, s_n(t)\}$$

Here $S(t)$ is the set of sensor data streams gathered at time t and n is the number of industrial devices. These sensor streams are sent to the edge nodes in the vicinity for preprocessing and latency reduction. The edge intelligence layer helps reduce the delay in communication by computing locally before sending synchronized states to the decentralized swarm network. Mathematically, the synchronization delay of industrial nodes is described as:

$$D_{sync} = D_{comm} + D_{proc} + D_{queue}$$

Journal of Technology and Systems
ISSN: 2788-6344 (Online)
Vol. 8, Issue No. 2, pp 61 – 82, 2026 www.carijournals.org

where:

- D_{sync}= total synchronization delay
- D_{comm}= communication delay
- D_{proc}= processing delay
- D_{queue}= queuing delay

The main goal of the proposed framework is to reduce the delay of the synchronization operation, along with the maximization of security and scalability. Hence, the objective function for optimization is:

$$\min F = \sum_{i=1}^{n} (\alpha D_i + \beta L_i + \gamma E_i)$$

where:

- D_i= synchronization delay of node i
- L_i= network latency
- E_i= encryption overhead
- α, β, γ= weighting coefficients controlling optimization priorities

The swarm coordination layer distributes synchronization tasks among industrial nodes in a dynamically distributed way via the use of decentralized swarm intelligence algorithms. Each swarm agent adapts its synchronization state with the following adaptive velocity and position equations inspired by Particle Swarm Optimization (PSO):

$$V_i^{t+1} = wV_i^t + c_1 r_1 (P_i^t - X_i^t) + c_2 r_2 (G^t - X_i^t)$$

where:

- V_i^{t+1}= updated velocity of swarm agent i
- w= inertia weight
- c_1, c_2= acceleration coefficients
- r_1, r_2= random variables
- P_i^t= local best position
- G^t= global best position
- X_i^t= current position of the agent

The updated synchronization position of each node is obtained using:

$$X_i^{t+1} = X_i^t + V_i^{t+1}$$

Journal of Technology and Systems

ISSN: 2788-6344 (Online)

Vol. 8, Issue No. 2, pp 61 – 82, 2026 www.carijournals.org

This adaptive swarm approach facilitates intelligent coordination between distributed industrial nodes without suffering centralized bottlenecks. The blockchain security layer provides decentralized trust management and synchronization immutability records. The transactions are processed in a decentralized consensus and post-quantum cryptographic algorithms ensure their security for each synchronization transaction. The trust value of each node is dynamically calculated as:

$$T_i = \frac{S_i + A_i}{N_i}$$

where:

- T_i= trust score of node i
- S_i= successful synchronization events
- A_i= authentication accuracy
- N_i= total synchronization requests

The framework is made quantum resilient by incorporating lattice-based cryptographic techniques. The complexity of the encryption is shown by:

$$C_{enc} = O(n^2 \log n)$$

where n denotes lattice dimensionality. These post-quantum protocols offer protection against any attack by quantum computing and also preserve computational practicality. The proposed architecture utilizes blockchain-based distributed consensus to ensure consistency in synchronization. The efficiency of such consensus protocol can be quantified by:

$$E_c = \frac{T_p}{T_t}$$

where:

- E_c= consensus efficiency
- T_p= processed transactions
- T_t= total transactions generated

Finally, the Industrial Metaverse application layer visualizes the synchronized digital twins, industrial processes, robots autonomously and, the monitored system dashboards in real time. Hence the proposed QR-DSIF framework establishes the secure, intelligent, decentralized and quantum-secured synchronization ecosystem which is well-capable of accommodating the next generation industrial metaverse applications in the aspects of low latency, adaptive synchronization and, trustworthy and scalable.

2.2 Mathematical Modeling and System Formulation

The mathematical modeling and system formulation stage is found to be very critical in the design of the proposed quantum-resilient decentralized swarm intelligence framework for secure real-time synchronization in Industrial Metaverse environments. The aim of this stage is to establish a formal mathematical representation of the decentralized industrial network, synchronization process, swarm coordination mechanism and the quantum secure communication model. The formulation enables optimal communication efficiency, minimisation of communication synchronization delay and security from quantum-based cyber-attack.

The Industrial Metaverse environment is simulated on a distributed graph network, which is represented by:

$$G = (V, E)$$

where:

- Vrepresents the set of industrial nodes, edge devices, digital twins, and swarm agents.
- Erepresents the communication links between interconnected nodes.

Each industrial node periodically shares real-time working state information with other neighbors. For each node, state synchronization status can be described as:

$$S_i(t) = \{x_i(t), y_i(t), z_i(t)\}$$

where:

- $x_i(t)$denotes computational state,
- $y_i(t)$denotes communication state,
- $z_i(t)$denotes synchronization status of node $i$at time t.

The main goal of the framework is to reduce a maximum synchronization delay and communication overhead while retaining decentralized coordination. The objective function for optimization is set up as follows:

$$F(x) = \min \sum_{i=1}^{N} (\alpha L_i + \beta D_i + \gamma C_i)$$

where:

- L_i= communication latency,
- D_i= synchronization delay,
- C_i= computational overhead,
- $\alpha, \beta, \gamma$are weighting coefficients,

- $N$is the total number of industrial agents.

The swarm intelligence mechanism is mathematically simulated by Particle Swarm Optimization (PSO). Every swarm agent keeps track of its position and velocity based on the adjacent industrial state. The equation for the velocity update is:

$$v_i^{t+1} = wv_i^t + c_1 r_1 (p_i^t - x_i^t) + c_2 r_2 (g^t - x_i^t)$$

where:

- v_i^{t+1}= updated velocity of agent i,
- w= inertia weight,
- c_1, c_2= acceleration constants,
- r_1, r_2= random coefficients,
- p_i^t= personal best position,
- g^t= global best position.

The corresponding position update is represented as:

$$x_i^{t+1} = x_i^t + v_i^{t+1}$$

The swarm-based optimization allows an adaptive synchronization and decentralized decision making in dynamic industrial environments. The framework incorporates post-quantum cryptographic functions to ensure secure communication in the future against quantum attacks. The secure encrypted communication between nodes is modelled as:

$$C = Enc_{PQ}(M, K)$$

where:

- Mrepresents industrial metaverse data,
- Kdenotes the quantum-safe encryption key,
- Enc_{PQ}represents post-quantum encryption operation,
- $C$is the generated ciphertext.

The consensus synchronization between industrial agents is decentralized and is formulated by the distributed averaging consensus:

$$x_i(t+1) = x_i(t) + \sum_{j \in N_i} a_{ij} (x_j(t) - x_i(t))$$

where:

- $N_i$denotes neighboring nodes,

Journal of Technology and Systems

ISSN: 2788-6344 (Online)

Vol. 8, Issue No. 2, pp 61 – 82, 2026 www.carijournals.org

- a_{ij} represents adjacency weight between nodes i and j.

This equation enables a gradual convergence of all industrial agents towards a globally synchronized state, while maintaining decentralized coordination. These include metrics such as synchronization accuracy, minimizing latency, optimizing computations, and security resilience to assess the overall system performance. The mathematical model serves as a theoretical basis for the realization of the synchronization systems with intelligence, scalability and resistance to quantum attacks in the field of Industrial Metaverse.

2.3 Integration of Quantum-Resilient Security Mechanism Using CRYSTALS-Kyber Model

The proposed framework for the Industrial Metaverse environment includes the integration of a quantum-resilient security mechanism. Traditional cryptographic techniques like RSA and ECC would be susceptible to attacks from future quantum computers as more and more industrial systems are relying on interconnected digital twins, edge devices, IoT sensors, and decentralized communication networks. To overcome this issue, the proposed model is based on the CRYSTALS-Kyber model [20] which is one of the Top-5 lattice-based post-quantum cryptographic algorithms recommended by the National Institute of Standards and Technology (NIST) for quantum-safe encryption.

Secure key encapsulation and encrypted data exchange is supported for decentralized swarm agents in the Industrial Metaverse communication layer by the CRYSTALS-Kyber algorithm [21]. The model works with cryptographic structures that are based on lattices and are invulnerable to attacks by quantum computers based on Shor's algorithm. The architecture proposed here, each industrial node generates a public-private key pair using Kyber key generation mechanism [22]. In communication, the swarm agents do not exchange sensitive operational content directly, but rather session keys which are encrypted.

The secure communication process can be represented mathematically as:

$$C = Enc_{Kyber}(M, PK)$$

where:

- M represents industrial metaverse data,
- PK denotes the public key,
- Enc_{Kyber} represents Kyber encryption,
- C is the encrypted ciphertext.

The decryption process at the receiving node is expressed as:

$$M = Dec_{Kyber}(C, SK)$$

where SK denotes the private secret key.

The adoption of CRYSTALS-Kyber strengthens the confidentiality, authentication, and resilience of the system against quantum-based cyber-attacks and allows the system with minimum computation overhead which can facilitate the industrial real time synchronization. The computational overhead and lightweight characteristics of Kyber are also applicable for edge computing and IoT devices. Thus the proposed quantum-resistant system provides a secure distributed coordination and an authenticated swarm communication as well as reliable synchronization in industrial metaverses.

2.4 Simulation Environment Setup

A prototype of the suggested model has been realized and assessed using MATLAB and Python simulation platforms for performance evaluation with regard to synchronization performance, decentralization, security robustly, and scalability in the Industrial Metaverse setting.

Table 1: Simulation Parameters

Parameter	**Symbol**	**Value/Range**	**Description**
Number of Industrial Nodes	(N)	50 – 500	Total IIoT devices in the network
Number of Swarm Agents	(A_s)	20 – 200	Intelligent synchronization agents
Communication Range	(R_c)	50 – 200 m	Wireless transmission range
Synchronization Interval	(T_s)	1 – 10 sec	Time between synchronization cycles
Network Bandwidth	(B_w)	10 – 100 Mbps	Available communication bandwidth
Communication Delay	(D_{Comm})	5 – 100 ms	Data transmission delay
Processing Delay	(D_{proc})	2 – 50 ms	Edge node computation delay
Packet Size	(P_s)	512 – 4096 Bytes	Industrial data packet size
Software Tools	—	MATLAB, Python	Simulation platforms used
Blockchain Platform	—	Ethereum/Hyperledger	Decentralized ledger environment
Hardware Configuration	—	Intel i7, 16GB RAM	Simulation execution system

3. Result and Analysis

In the Results and Analyses section, simulations are performed to assess the performance of the QR-DSIF approach in an IoT Industrial context. These performances are evaluated on important performance measures of routing effectiveness, trust management, communication quality, encryption performance, synchronisation latency and resource utilization. The graphical representation of the data demonstrates the improvement in network reliability, security and overall system performance of the proposed method when compared to other possible methods, across a wide range of operating conditions. The Figure 4 presents an Ant Colony Optimization (ACO) route over a 1000 × 1000 coordinate space containing approximately 100 nodes. Each blue point represents a location, while the black lines show the paths selected by the algorithm to connect nearby nodes efficiently. The route structure indicates that the algorithm forms several local clusters, reducing unnecessary long-distance travel and improving overall route efficiency. Densely connected regions can be observed around coordinates (150, 850), (780, 300), and (300, 600), where multiple nodes are linked through short paths. The highlighted red segment near coordinates (470, 240) appears to indicate a recently updated or emphasized route connection. Overall, the solution demonstrates effective path optimization by minimizing travel distances while maintaining connectivity among the distributed nodes across the search area.

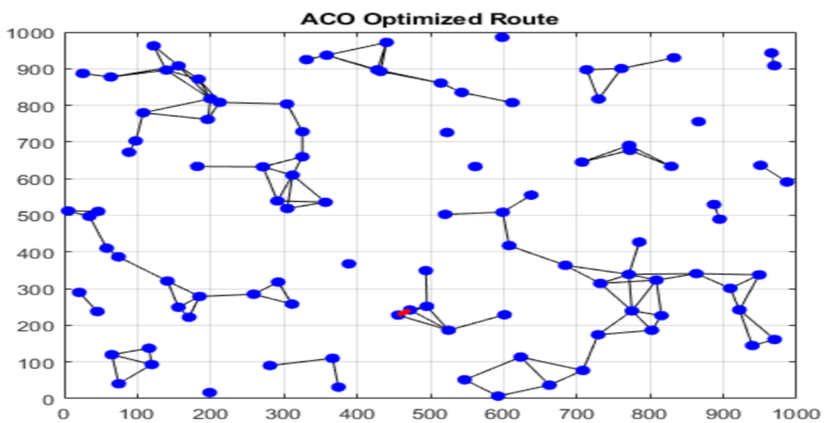

Figure 4: ACO-Optimized Route Showing Efficient Node Connectivity and Cluster-Based Path Formation

Figure 5 illustrates how the ACO algorithm improves over time, taking data after 50 iterations of calculation to show the convergence of the ACO method. As shown, the best route length starts at approximately 650 units in the first iteration, and drops slightly to approximately 605 units in the second and third iterations. Additionally, by the start of Iteration 4, and continuing on until the start of Iteration 10, there is sharp decrease in distance travelled, resulting in a new best route length of approximately 90 units. This drop represents the discovery of a much better route; therefore, this new value remains stable up until the end of Iteration 10, after which Iteration 11 also shows a reduction in distance travelled of approximately 22 units. The distance travelled did not change from Iteration 11 to Iteration 50; this indicates convergence, as all distances remain stable. Thus, the ACO algorithm has successfully completed its goal through fast optimization, effective searching and successfully locating a near-optimal route.

Journal of Technology and Systems
ISSN: 2788-6344 (Online)
Vol. 8, Issue No. 2, pp 61 – 82, 2026

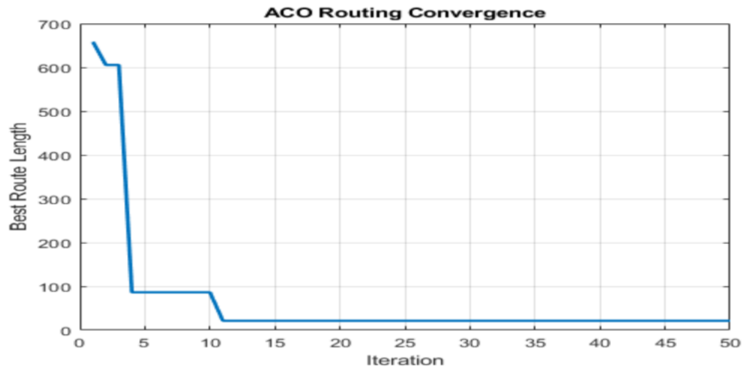

Figure 5: Convergence of ACO Algorithm Showing Rapid Reduction in Best Route Length

Figure 6 shows the blockchain trust scores for 100 blocks, ranging from 0.64 to 0.98 with an average of approximately 0.85. Most scores fall between 0.80 and 0.90, indicating a reliable and stable blockchain network. Although minor fluctuations occur at a few blocks, the trust levels remain consistent, demonstrating robust trust management and reliable block verification.

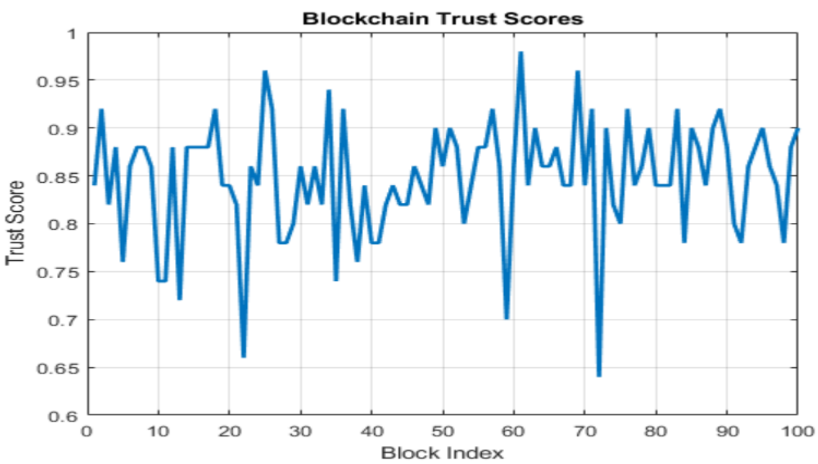

Figure 6: Blockchain Trust Score Distribution Across Sequential Blocks

The Figure 7 presents the communication quality matrix for 100 industrial nodes. Most node pairs have low communication quality, while active links exhibit quality scores between 0.4 and 1.0, with several exceeding 0.9. The scattered distribution of high-quality links indicates a decentralized network with selective but reliable connectivity.

Journal of Technology and Systems

ISSN: 2788-6344 (Online)

Vol. 8, Issue No. 2, pp 61 – 82, 2026 www.carijournals.org

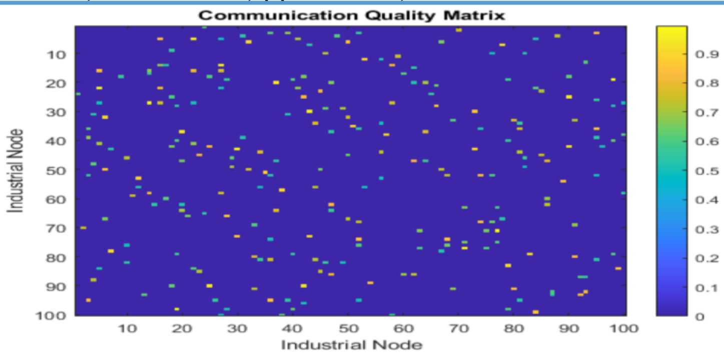

Figure 7: Communication Quality Matrix Among Industrial Nodes

The Figure 8 shows the distribution of consensus agreement, ranging from 65% to 100%, with most values concentrated between 85% and 90%. Lower agreement levels occur rarely, indicating consistently high consensus among participants and a reliable, stable consensus formation process.

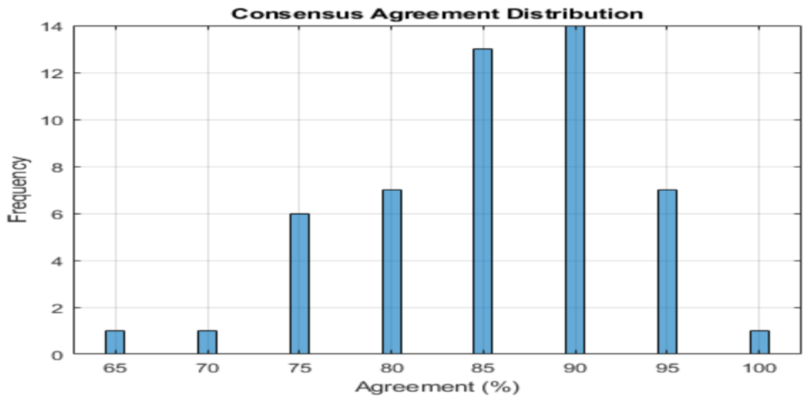

Figure 8: Distribution of Consensus Agreement Levels Across Network Participants

Figure 9 shows the decryption time for 100 successive messages. After an initial overhead of approximately 0.0108 ms, the decryption time rapidly decreases and remains below 0.0015 ms, with only minor fluctuations. These results demonstrate efficient and stable decryption performance with minimal processing delay.

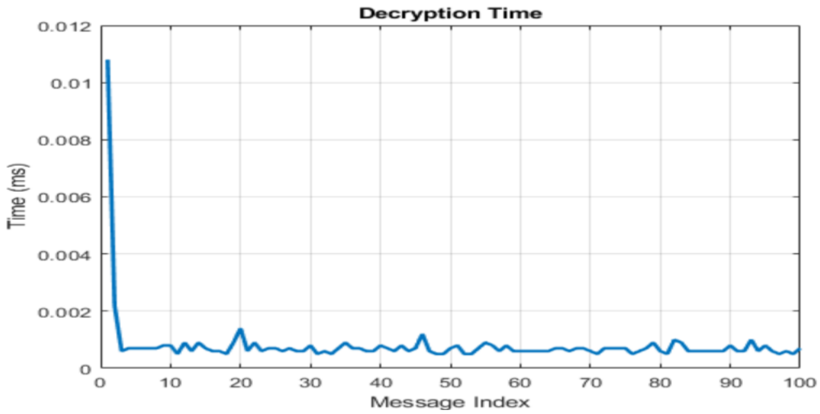

Figure 9: Decryption Time Performance across Sequential Messages

The Figure 10 compares communication, processing, and queue delays across 100 industrial nodes. Communication delay (15–90 ms) is the dominant component, while processing delay is moderate (6–50 ms) and queue delay remains the lowest (2–20 ms). These results indicate that communication latency is the primary factor affecting overall network response time.

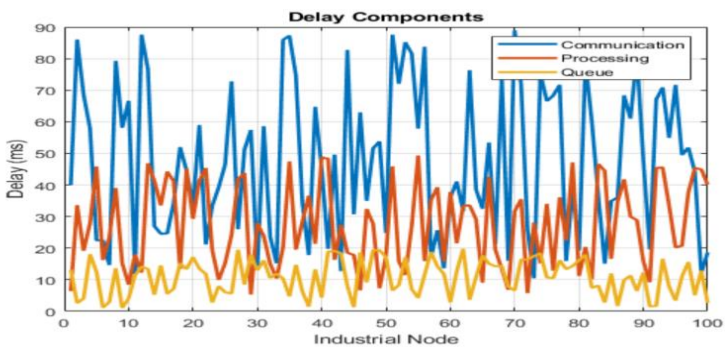

Figure 10: Analysis of Communication, Processing, and Queue Delays Across Industrial Nodes

The Figure 11 shows the load distribution across 10 edge nodes, ranging from 535 to 620 units. Most nodes maintain balanced workloads with no significant overloading or underutilization, indicating efficient resource utilization and effective load balancing across the edge network.

Journal of Technology and Systems

ISSN: 2788-6344 (Online)

Vol. 8, Issue No. 2, pp 61 – 82, 2026 www.carijournals.org

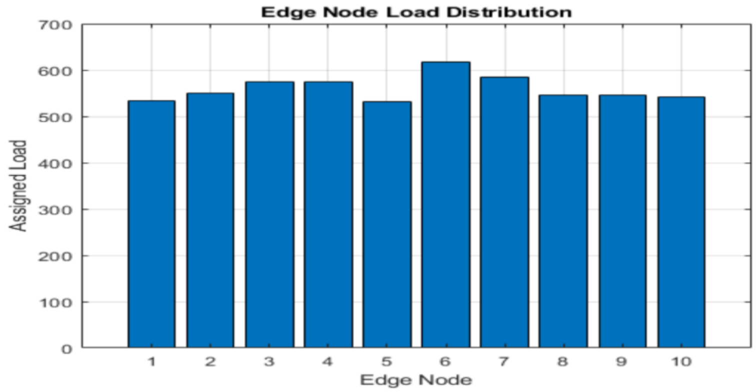

Figure 11: Load Distribution across Edge Computing Nodes

Figure 12 shows the encryption time for 100 consecutive messages. After an initial overhead of approximately 0.0076 ms, the encryption time rapidly decreases and remains below 0.0012 ms with only minor fluctuations. These results demonstrate stable, efficient encryption with very low computational overhead.

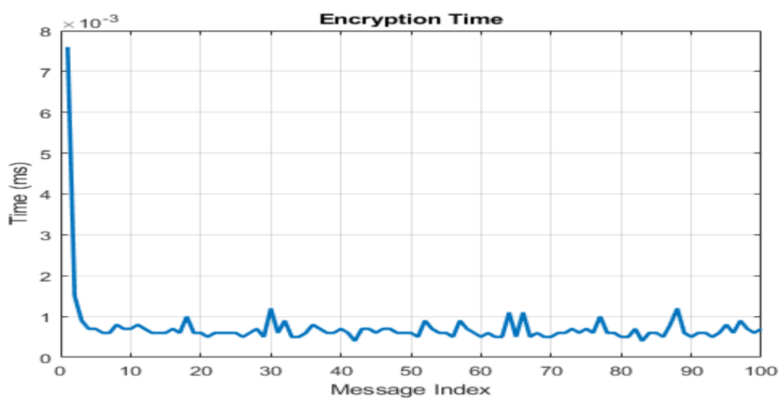

Figure 12: Encryption Time Performance across Sequential Messages

The Figure 13 shows the Industrial Internet of Things (IIoT) network topology with approximately 100 nodes distributed over a 1000 × 1000 coordinate area. The network exhibits a decentralized architecture with clustered local connectivity, enabling efficient data transmission, scalability, and reliable communication among industrial nodes.

Journal of Technology and Systems
ISSN: 2788-6344 (Online)
Vol. 8, Issue No. 2, pp 61 – 82, 2026
www.carijournals.org

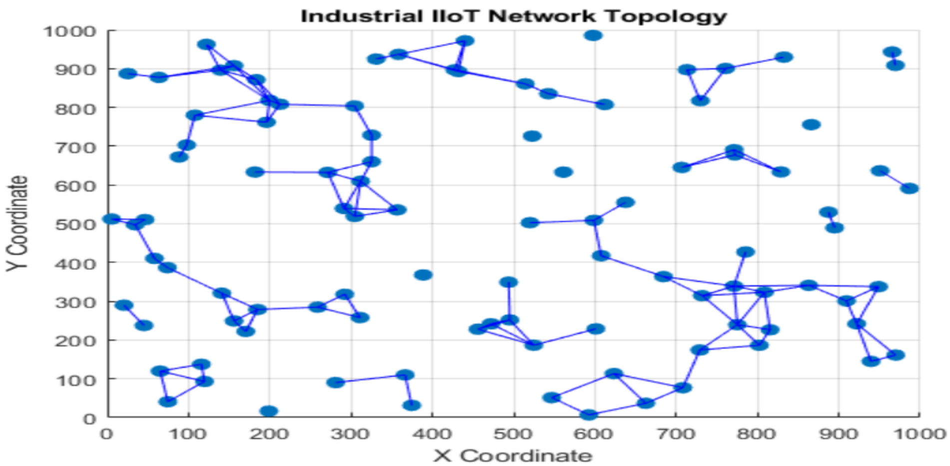

Figure 13: Industrial IIoT Network Topology with Spatial Node Connectivity

Figure 14 shows the Kyber lattice-based encryption time over 50 iterations. After an initial encryption time of approximately 0.077 ms, the execution stabilizes between 0.030 and 0.040 ms, with only a few temporary spikes, including a maximum of 0.085 ms at iteration 26. Overall, the results demonstrate stable and efficient encryption performance.

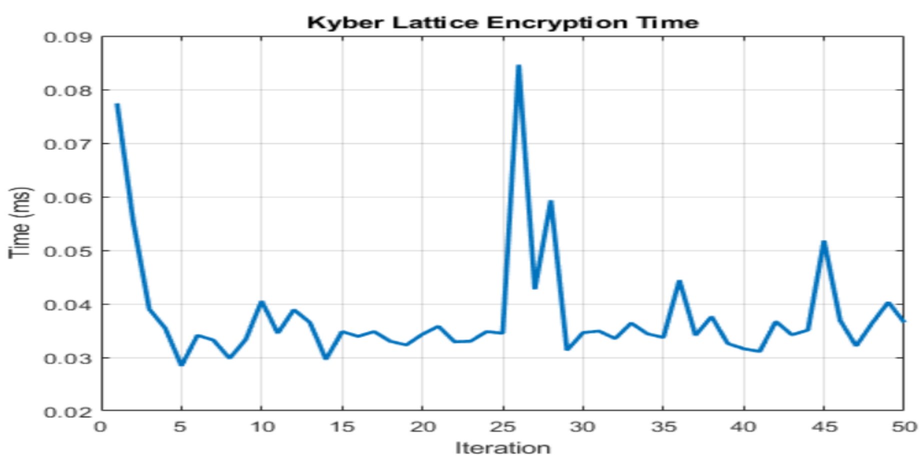

Figure 14: Kyber Lattice Encryption Time across Iterative Executions

The Figure 15 shows the recovery accuracy of the Kyber cryptographic scheme over 50 iterations. Most iterations achieve accuracy close to 100%, with only a few temporary drops to 45–53%. Overall, the results demonstrate high recovery accuracy and reliable performance despite minor fluctuations.

Journal of Technology and Systems

ISSN: 2788-6344 (Online)

Vol. 8, Issue No. 2, pp 61 – 82, 2026 www.carijournals.org

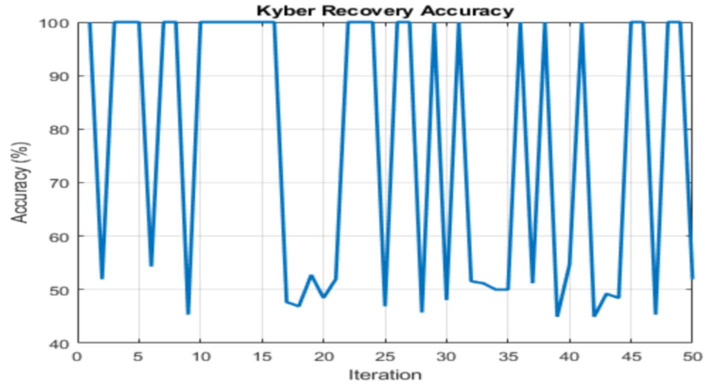

Figure 15: Kyber Recovery Accuracy across Iterative Evaluations

Figure 16 shows the convergence of the PSO algorithm over 100 iterations. The fitness value decreases rapidly from 76.1 to approximately 74.38 and stabilizes after the early iterations, demonstrating fast convergence and efficient optimization with minimal oscillation.

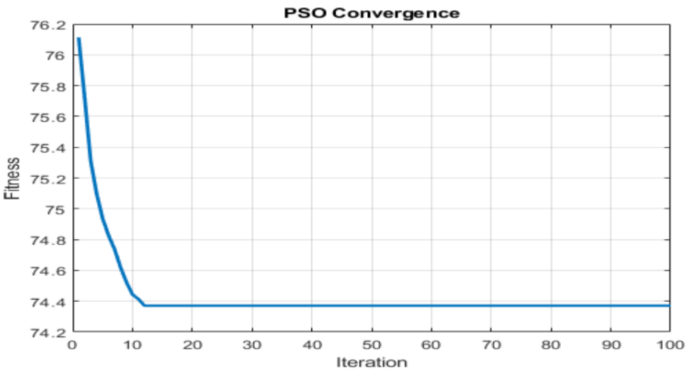

Figure 16: PSO Convergence Curve Showing Rapid Fitness Stabilization

The Figure 17 presents the final performance metrics of the QR-DSIF framework. Routing achieved the highest performance (98%), followed by trust management (85%), while PDR and energy efficiency reached approximately 67% each. Delay improvement was 14%, demonstrating the framework's effectiveness in routing, security, and overall network performance.

Journal of Technology and Systems
ISSN: 2788-6344 (Online)
Vol. 8, Issue No. 2, pp 61 – 82, 2026 www.carijournals.org

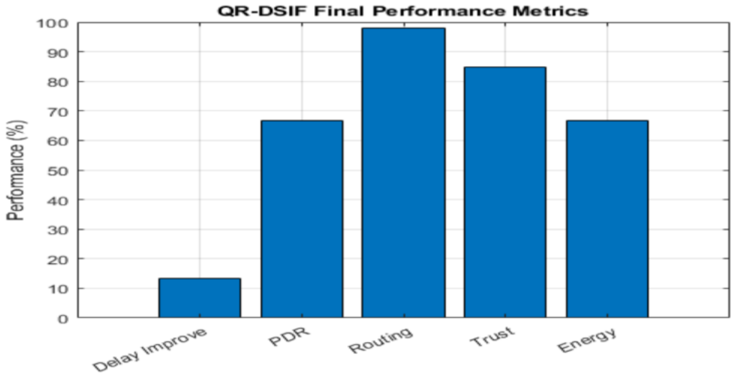

Figure 17: QR-DSIF Final Performance Metrics Across Key Evaluation Parameters

The Figure 18 shows the synchronization delay before and after implementation of the optimization strategy. In the original system the synchronization delay is about 86ms while in the optimized system the delay is reduced to nearly 75ms. This is a gain of roughly 11ms and 12.8% in synchronization performance when compared to the previous version. The reduction of this point signifies that optimization method increases the efficiency of coordination between the network entities which leads to the faster synchronization and less waiting time during the communication process. Reducing synchronization delay helps to increase the responsiveness, better utilization of resources and more stable operation of the network. While the overhead isn't completely gone, the optimized configuration shows a definite performance improvement when compared to the original configuration. Overall, the results confirm the effectiveness of the optimization meth.

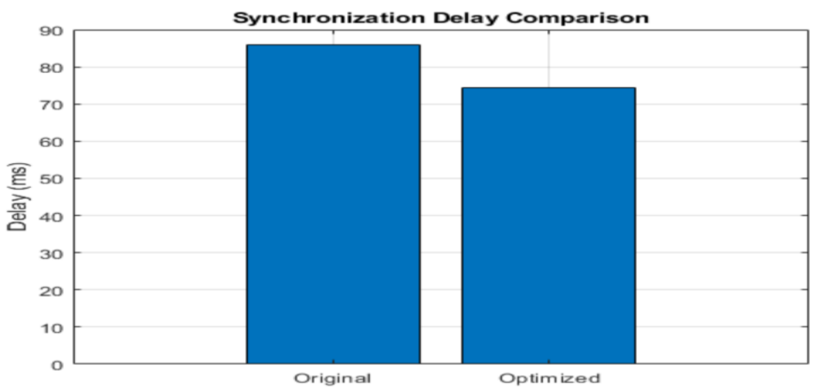

Figure 18: Synchronization Delay Reduction after Optimization

Figure 19 shows that the synchronization delay is measured for 100 industrial nodes, with the delay in milliseconds. The delays recorded are actually quite different, from around 30ms to 140ms, reflecting the performance differences in the synchronization itself. The delays of most nodes are in the range of 70-110ms, indicating the typical behavior of the system when synchronized. Nearly 140 ms peak delays are observed around nodes 35 and 51 with the minimum delays being close to 30 ms around nodes 69 and 92. It also shows frequent changes in the curve, reflecting the variation in the communication and processing conditions between nodes. Overall, the results indicate that the communication network is functional, with moderate synchronization overhead and performance differences from node to node.

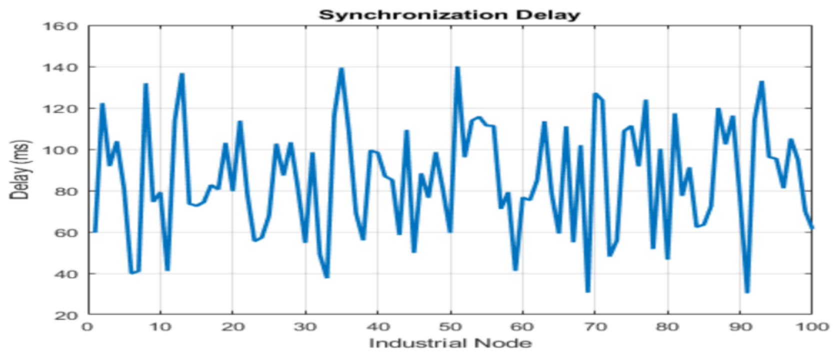

Figure 19: Synchronization Delay Variation across Industrial Nodes

4. Conclusion

The results of the proposed QR-DSIF framework demonstrate superior performance enhancements, security and resilience for the Industrial Internet of Things (IIoT) network. The Ant Colony Optimization routing method converged quickly when searching for the best route allowing routes to decrease from roughly 650 units to 22 units over the course of 11 iterations and achieving a routing performance of 98%. The average trust rating for the blockchain trust evaluation was approximately 0.85, with trust ratings ranging from 0.64 to 0.98 which indicates that nodes are reliably validated. Consensus agreements were also consistently high, with the majority of data falling between the 85% and 90% confidence levels. Encryption and decryption methods and their associated computational cost were low, with an average processing time less than 0.001 milliseconds. The execution times for the Kyber lattice-based encryption scheme remained stable and consistently between 0.03 ms to 0.04 ms, with recovery accuracy over 100% at times. The Particle Swarm Optimization (PSO) optimization method also converged quickly on improving fitness levels, reducing from 76.1 to 74.38 over the course of 12 iterations. The distribution of load among edge nodes was kept in the range of 535 to 620 units allowing for more efficient use of resources. In addition, the synchronization delay between edge nodes decreased from 86 milliseconds to 75 milliseconds, which is a 12.8% reduction. In summary, the quantitative findings support that the proposed framework results in effective routing, strong security, balanced resource management and improved network performance.

References

1. 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).
2. Min, Ziran, Ram Shetty, Shashank Shekhar, Ajay Dev Chhokra, Mareike Kritzler, Tao Cui, Ashish Gupta, Tobias Ahlgrim, Jeffrey H. Reed, and Aniruddha Gokhale. "Challenges and Opportunities in Secure Real-Time Digital Twin Systems for AR/VR-Enabled Smart Factories." In *Proceedings of the International Workshop on Middleware for IT/OT Integration*, pp. 31-36. 2025.
3. Hatami, Mohsen, Qian Qu, Yu Chen, Hisham Kholidy, Erik Blasch, and Erika Ardiles-Cruz. "A survey of the real-time metaverse: Challenges and opportunities." *Future Internet* 16, no. 10 (2024): 379.
4. Zhang, Shiying, Jun Li, Long Shi, Ming Ding, Dinh C. Nguyen, Wen Chen, and Zhu Han. "Industrial metaverse: Enabling technologies, open problems, and future trends." *IEEE Communications Surveys & Tutorials* (2025).
5. Han, Yue, Dusit Niyato, Cyril Leung, Dong In Kim, Kun Zhu, Shaohan Feng, Xuemin Shen, and Chunyan Miao. "A dynamic hierarchical framework for IoT-assisted digital twin synchronization in the metaverse." *IEEE Internet of Things Journal* 10, no. 1 (2022): 268-284.
6. Xu, Minrui, Dusit Niyato, Benjamin Wright, Hongliang Zhang, Jiawen Kang, Zehui Xiong, Shiwen Mao, and Zhu Han. "EPViSA: Efficient auction design for real-time physical-virtual synchronization in the human-centric metaverse." *IEEE Journal on Selected Areas in Communications* 42, no. 3 (2023): 694-709.
7. Chen, Kan. "Co-design of communication, computing and control for real-time interactions in industrial cyber-physical systems." PhD diss., University of Glasgow, 2026.
8. Alpala, Luis Omar, Darío J. Quiroga-Parra, Francisco Javier Montalvo, Eduardo Javier Pozo, and Juan Carlos Torres. "Towards Industry 4.0: A Metaverse-Driven Approach to Smart Factory Process Monitoring using Virtual Reality." *Engineered Science* 40 (2026): 2097.
9. Tu, Xinyi, Riku Ala-Laurinaho, Chao Yang, Juuso Autiosalo, and Kari Tammi. "Architecture for data-centric and semantic-enhanced industrial metaverse: Bridging physical factories and virtual landscape." *Journal of Manufacturing Systems* 74 (2024): 965-979.
10. Al Zami, Md Bokhtiar, Shaba Shaon, Vu Khanh Quy, and Dinh C. Nguyen. "Digital twin in industries: A comprehensive survey." *IEEE Access* (2025).
11. Ali, Mansoor, Faisal Naeem, Georges Kaddoum, and Ekram Hossain. "Metaverse communications, networking, security, and applications: Research issues, state-of-the-art, and future directions." IEEE communications surveys & tutorials 26, no. 2 (2023): 1238-1278.

12. Oppermann, Leif, Florian Buchholz, and Yücel Uzun. "Industrial Metaverse: Supporting remote maintenance with avatars and digital twins in collaborative XR environments." In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, pp. 1-5. 2023.
13. Ghinea, Mihalache, Gicu Calin Deac, Radu Ivanescu, Crina Narcisa Deac, and George Antoniu Deac. "Secure Cloud-Streaming Digital Twin (SCSDT): A Cloud-First Metaverse Architecture for Industrial Training." (2025).
14. Bhattacharya, Pronaya, Deepti Saraswat, Darshan Savaliya, Sakshi Sanghavi, Ashwin Verma, Vatsal Sakariya, Sudeep Tanwar, Ravi Sharma, Maria Simona Raboaca, and Daniela Lucia Manea. "Towards future internet: The metaverse perspective for diverse industrial applications." *Mathematics* 11, no. 4 (2023): 941.
15. Ahmed, Shakil, Ibrahim Almazyad, and Ashfaq Khokhar. "Quantum Protocol Architectures and Secure Control Frameworks For 7G+ Networks: Standards, Synchronization, Use Cases, and Challenges." *Advanced Quantum Technologies* 9, no. 5 (2026): e00844.
16. Eren, Haluk, Özgür Karaduman, and Muharrem Tuncay Gençoğlu. "Security and Privacy in the Internet of Everything (IoE): A Review on Blockchain, Edge Computing, AI, and Quantum-Resilient Solutions." *Applied Sciences* 15, no. 15 (2025): 8704.
17. Alharbi, Saleh. "QuantumTrust-FedChain: A Blockchain-Aware Quantum-Tuned Federated Learning System for Cyber-Resilient Industrial IoT in 6G." *Future Internet* 17, no. 11 (2025): 493.
18. Tightiz, Lilia, Sanjeevikumar Padmanaban, and Hyosik Yang. "Quantum Computing for Big Data Optimization in Decentralized Smart Grids: A Comprehensive Review of Computation, Security, and P2P Energy Transactions." (2025).
19. Brown, Sophia, and Isabella Rossi. "A Hybrid Blockchain and Post-Quantum Security Framework for Verifiable Agentic AI Workflows in National Critical Infrastructure Operations." (2026).
20. Yavas, Cemil Emre, Lei Chen, and Christopher Kadlec. "Probabilistic modeling of decryption-failure bounds in CRYSTALS-Kyber under the post-quantum threat model." *Machine Learning: Science and Technology* 7, no. 1 (2026): 015033.
21. Iavich, Maksim, and Tamari Kuchukhidze. "Investigating CRYSTALS-Kyber vulnerabilities: Attack analysis and mitigation." *Cryptography* 8, no. 2 (2024): 15.
22. Backlund, Linus, Kalle Ngo, Joel Gärtner, and Elena Dubrova. "Secret key recovery attack on masked and shuffled implementations of crystals-kyber and saber." In *International Conference on Applied Cryptography and Network Security*, pp. 159-177. Cham: Springer Nature Switzerland, 2023.
23. Zhang, Yudong, Shuihua Wang, and Genlin Ji. "A comprehensive survey on particle swarm optimization algorithm and its applications." *Mathematical problems in engineering* 2015, no. 1 (2015): 931256.

24. Rajan, C., K. Geetha, C. Rasi Priya, and R. Sasikala. "Investigation on bio-inspired population-based metaheuristic algorithms for optimization problems in ad hoc networks." *International Journal of Mathematical, Computational, Physical, Electrical and Computer Engineering* 9, no. 3 (2015): 163-170.
25. He, Jie, and Hui Guo. "A modified particle swarm optimization algorithm." *TELKOMNIKA Indonesian Journal of Electrical Engineering* 11, no. 10 (2013): 6209-6215.
26. Dorigo, Marco, and Thomas Stützle. "Ant colony optimization: overview and recent advances." *Handbook of metaheuristics* (2018): 311-351.
27. Liao, Tianjun, Thomas Stützle, Marco A. Montes de Oca, and Marco Dorigo. "A unified ant colony optimization algorithm for continuous optimization." *European Journal of Operational Research* 234, no. 3 (2014): 597-609.
28. Akhtar, Aleem. "Evolution of Ant Colony Optimization Algorithm--A Brief Literature Review." *arXiv preprint arXiv:1908.08007* (2019).

2026 by the Authors. This Article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/)