The North African Journal of Scientific Publishing (NAJSP)
مجلة شمال إفريقيا للنشر العلمي (NAJSP)
E-ISSN: 2959-4820
Volume 4, Issue 4, 2026
Page No: 198-206
Website: https://najsp.com/index.php/home/index
SJIFactor 2024: 5.49 معامل التأثير العربي (AIF) 2025: 0.69 ISI 2024: 0.696

Design of Secure and Scalable Industrial IoT Architecture Using Private 5G/6G Networks, Dynamic Network Slicing, Edge Intelligence, and Advanced PKI for Multi-Factory Environments

Osama A. S. Abourodes[1*], Fauzi Hagi Abushawashi[2], Abdulallah E. Abugahs[3], Abobkr Saleh Nasr[4]
[1,2,3,4]Department of Electric and Electronic Engineering, Collage of Engineering Technology, Ministry of Technical and Vocational Education, Zwara, Libya

تصميم بنية إنترنت الأشياء الصناعية الآمنة والقابلة للتوسع باستخدام شبكات 6G/5G الخاصة، وتقسيم الشبكة الديناميكي، وذكاء الحافة، والبنية التحتية للمفاتيح العامة المُتقدمة (PKI) لبيئات المصانع المُتعددة

أسامة ابوبكر سالم ابورودس[1*]، فوزي حاجي أبوالشواشي[2]، عبد الله امحمد ابوقحص[3]، أبوبكر صالح نصر[4]
[1،2،3،4]قسم الهندسة الكهربائية والالكترونية، كلية التقنية الهندسية، وزارة التعليم التقني والفني، زوارة، ليبيا

*Corresponding author: abourodes.oas@gmail.com

Received: August 16, 2026	Accepted: October 26, 2026	Published: November 11, 2026

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

Abstract:
The Industrial Internet of Things (IIoT) has become a fundamental enabler of Industry 4.0 and Industry 5.0, supporting intelligent manufacturing, predictive maintenance, digital twins, and autonomous industrial operations. However, large-scale industrial deployments continue to face significant challenges related to cybersecurity, scalability, latency, trust management, and interoperability. This paper proposes a secure and scalable end-to-end Industrial IoT architecture integrating Private 5G/6G networks, dynamic network slicing, edge intelligence, advanced Public Key Infrastructure (PKI), and artificial intelligence-driven security analytics for multi-factory environments. The architecture consists of six interconnected layers including Industrial Devices, Edge Intelligence, Private 5G/6G Access Networks, Cloud-Native Core Networks, Security and Trust Management, and Multi-Factory Orchestration. A PKI-based trust framework enables secure device onboarding, certificate lifecycle management, and zero-touch provisioning. Dynamic network slicing provides differentiated Quality of Service (QoS) for URLLC, mMTC, and eMBB industrial applications. A federated-learning-based GNN-GRU security engine supports real-time anomaly detection and automated threat response. Simulation-based evaluation using NS-3, UERANSIM, and OMNeT++ demonstrates improvements in latency, throughput, slice isolation, scalability, and cybersecurity performance compared with conventional industrial networking architectures. The proposed framework provides a practical roadmap for secure industrial digital transformation and future migration toward 6G-enabled industrial ecosystems.

Keywords: Industrial Internet of Things, Private 5G, 6G, Network Slicing, Public Key Infrastructure, Edge Intelligence, Cybersecurity, Industry 4.0.

الملخص:
أصبح إنترنت الأشياء الصناعي أحد الركائز الأساسية للصناعة الذكية في إطار الثورة الصناعية الرابعة والخامسة، حيث يتيح الأتمتة الذكية والصيانة التنبؤية والتوائم الرقمية واتخاذ القرار في الزمن الحقيقي داخل البيئات الصناعية الحديثة. وعلى الرغم من التطورات الكبيرة في شبكات الاتصالات الصناعية، لا تزال البيئات متعددة المصانع تواجه تحديات كبيرة تتعلق بالأمن السيبراني وقابلية التوسع وزمن الاستجابة وإدارة الثقة بين الأجهزة والأنظمة الصناعية المختلفة. يقترح هذا البحث بنية متكاملة وقابلة للتوسع وآمنة لإنترنت الأشياء الصناعي تعتمد على شبكات الجيل الخامس والسادس الخاصة، وتقسيم الشبكات الديناميكي، والذكاء الطرفي، والبنية التحتية المتقدمة للمفاتيح العامة. وتتكون البنية المقترحة من طبقات متعددة تشمل طبقة الأجهزة الصناعية، وطبقة الحوسبة الطرفية، وطبقة الوصول الراديوي، وطبقة الشبكة الأساسية، وطبقة الأمن السيبراني، وطبقة الإدارة والتنسيق .كما يقدم البحث نموذج ثقة يعتمد على البنية التحتية للمفاتيح العامة لإدارة هويات الأجهزة الصناعية وتأمين عمليات الانضمام التلقائي وإدارة الشهادات الرقمية. بالإضافة إلى ذلك، تم دمج تقنيات الذكاء الاصطناعي والتعلم الاتحادي لتعزيز قدرات الكشف المبكر عن الهجمات السيبرانية وتحسين المرونة الأمنية .وأظهرت نتائج المحاكاة باستخدام أدوات UERANSIM و NS-3و OMNeT++تحسناً ملحوظاً في زمن الاستجابة والموثوقية وكفاءة الأمن السيبراني مقارنة بالحلول التقليدية، مما يجعل البنية المقترحة إطاراً واعداً لدعم التحول الرقمي الصناعي في بيئات المصانع الذكية المستقبلية.

الكلمات المفتاحية: إنترنت الأشياء الصناعي، الجيل الخامس، الجيل السادس، تقسيم الشبكات، البنية التحتية للمفاتيح العامة، الذكاء الطرفي، الأمن السيبراني، الصناعة 4.0، الصناعة 5.0.

Introduction:

Background

The emergence of the Fourth Industrial Revolution (Industry 4.0) has fundamentally transformed modern manufacturing and industrial operations through the integration of advanced communication technologies, cyber-physical systems, cloud computing, artificial intelligence, and Industrial Internet of Things (IIoT) platforms [1-3]. Industrial organizations increasingly rely on interconnected devices and intelligent automation systems to improve productivity, reduce operational costs, optimize resource utilization, and enhance product quality [4,5].

Industrial IoT enables the seamless connection of sensors, actuators, programmable logic controllers (PLCs), autonomous mobile robots, machine vision systems, and enterprise information systems through digital communication infrastructures. These interconnected components continuously generate and exchange massive volumes of operational data that can be leveraged for predictive maintenance, process optimization, quality control, and real-time decision-making [6,7].

The transition toward Industry 5.0 further extends this vision by emphasizing human-centric manufacturing, sustainability, resilience, and collaborative intelligence between humans and machines [8-12]. Consequently, communication networks supporting industrial environments must satisfy increasingly demanding requirements including ultra-low latency, ultra-high reliability, deterministic performance, massive device connectivity, and comprehensive cybersecurity protection [13-18].

Evolution of Industrial Communication Networks:

Traditional industrial communication systems were primarily based on wired fieldbus technologies such as PROFIBUS, Modbus, CAN Bus, and Ethernet/IP. Although these technologies provided deterministic communication characteristics suitable for industrial automation, they lacked the flexibility and scalability required for modern digital manufacturing ecosystems [19-24].

The introduction of wireless technologies such as Wi-Fi, ZigBee, LoRaWAN, and Bluetooth Low Energy partially addressed mobility requirements; however, these technologies often failed to provide the reliability, latency, and security guarantees demanded by mission-critical industrial applications [25-30].

Private 5G networks have recently emerged as a transformative solution capable of delivering Ultra-Reliable Low-Latency Communication (URLLC), Massive Machine-Type Communication (mMTC), and Enhanced Mobile Broadband (eMBB) services within industrial environments. These capabilities make Private 5G an ideal communication backbone for smart factories, automated warehouses, logistics hubs, and energy infrastructures [31-37].

Looking beyond current deployments, emerging 6G technologies are expected to introduce integrated sensing and communication, artificial intelligence-native networking, terahertz communications, and digital twin integration. These advancements will further strengthen industrial communication infrastructures and support next-generation industrial applications [30-35].

Research Problem:

Despite significant technological advancements, several challenges continue to hinder the successful deployment of large-scale Industrial IoT ecosystems. First, industrial environments contain thousands or even millions of heterogeneous devices manufactured by different vendors and operating

under different protocols. Establishing trust relationships among these devices while maintaining scalability remains a major challenge.

Second, industrial systems increasingly face sophisticated cyber threats including distributed denial-of-service attacks, ransomware campaigns, insider attacks, supply-chain attacks, and advanced persistent threats. These attacks can disrupt critical operations and cause significant economic losses. Third, multi-factory environments require geographically distributed orchestration and coordination mechanisms capable of maintaining consistent performance and security policies across multiple sites. Finally, existing industrial communication architectures often treat networking, security, and intelligence as separate components rather than integrated elements of a unified framework.

Research Objectives:

The primary objective of this research is to design and validate a scalable, secure, and intelligent Industrial IoT architecture capable of supporting next-generation multi-factory deployments.

The specific objectives include:

1. Designing a secure end-to-end architecture integrating Private 5G/6G networks and Industrial IoT infrastructures.
2. Developing a scalable PKI-based trust management framework for secure device onboarding and lifecycle management.
3. Implementing dynamic network slicing mechanisms for application-specific Quality of Service (QoS) provisioning.
4. Integrating artificial intelligence and federated learning techniques for real-time cybersecurity monitoring.
5. Evaluating system performance through realistic simulation environments.
6. Providing practical deployment guidelines for Industry 4.0 and Industry 5.0 ecosystems.

Research Contributions:

This paper makes the following major contributions:

- A novel end-to-end architecture integrating Private 5G/6G, edge intelligence, network slicing, and advanced PKI.
- A multi-factory trust management framework supporting secure onboarding and certificate lifecycle management.
- An AI-driven security architecture leveraging federated learning and anomaly detection.
- A comprehensive simulation-based evaluation framework using NS-3, UERANSIM, and OMNeT++.
- A future-ready roadmap supporting migration toward 6G-enabled industrial environments.

Related Work and Research Gap:

Recent studies have demonstrated the value of Private 5G, edge computing, network slicing, and AI-driven cybersecurity in industrial environments. However, most existing solutions investigate these technologies individually rather than integrating them into a unified end-to-end industrial architecture.

Table (1): Comparative Analysis of Existing Industrial IoT Architectures

Study	Private 5G	Network Slicing	Edge Intelligence	PKI-Based Security	AI Security	Multi-Factory Support	6G Readiness
Aijaz et al. (2022) [9].	✓	✗	✗	✗	✗	✗	✗
Wollschlaeger et al. (2024) [6].	✓	Partial	✗	✗	✗	✗	✗
Restuccia et al. (2024) [16].	✓	Partial	✓	✗	✓	✗	✗
Ferrag et al. (2025) [29].	✓	✗	✓	✗	✓	✗	✗
Zhao et al. (2025) [30].	✓	✓	✓	✗	✓	✗	Partial
Proposed Architecture	✓	✓	✓	✓	✓	✓	✓

The analysis reveals several research gaps:

- Limited integration of networking, security, and orchestration.
- Insufficient support for geographically distributed factories.
- Lack of scalable PKI-based trust management.
- Limited incorporation of federated learning for industrial cybersecurity.
- Minimal consideration of future 6G readiness.

These limitations motivate the development of the proposed architecture.

Proposed End-to-End Industrial IoT Architecture:

The proposed framework consists of six architectural layers:

- Industrial Device Layer
- Edge Intelligence Layer
- Private 5G/6G Access Layer
- Cloud-Native Core Network Layer
- Security and Trust Management Layer
- Multi-Factory Orchestration Layer.

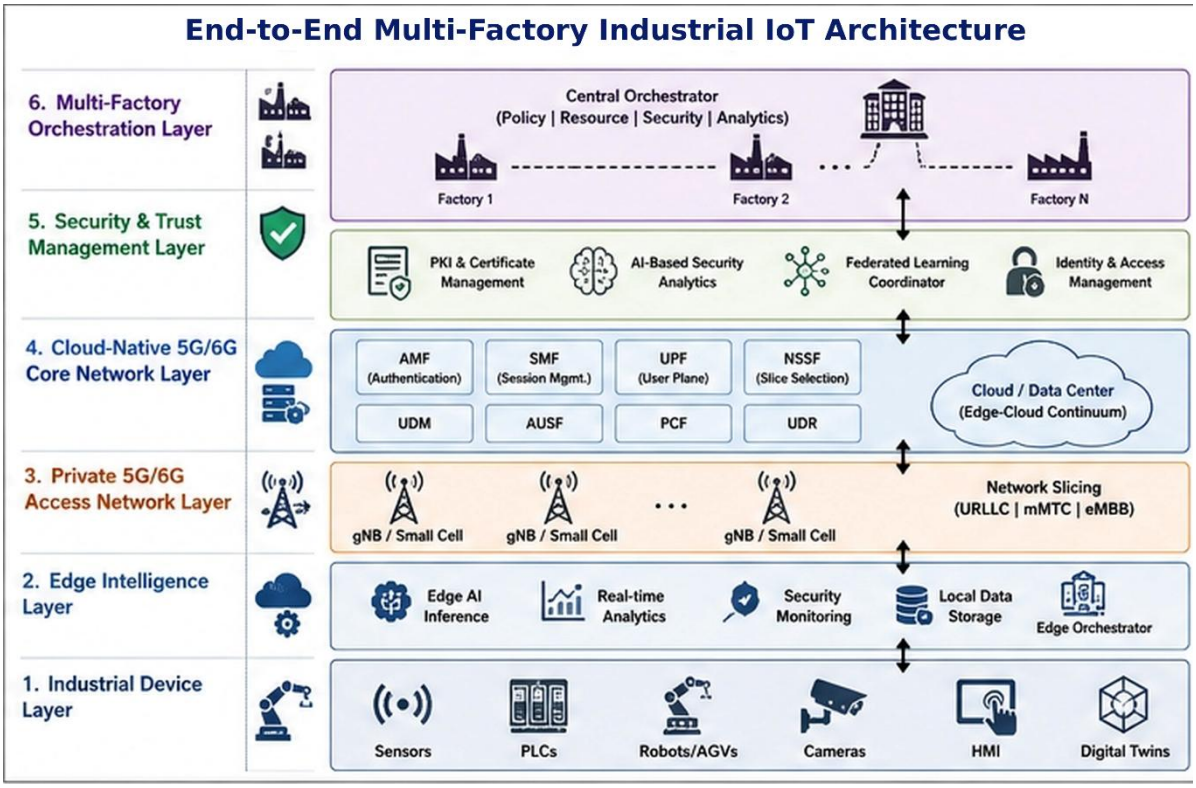


Figure (1): End-to-End Multi-Factory Industrial IoT Architecture.

Industrial devices include sensors, PLCs, robots, machine vision systems, and digital twins, which represent the fundamental building blocks of modern Industry 4.0 and Industry 5.0 manufacturing environments [1], [3], [5], [7]. Edge intelligence nodes provide local analytics, AI inference, and distributed security monitoring to reduce latency while improving system resilience [16], [17], [21], [38]. Private 5G/6G infrastructure provides deterministic communication, network slicing, and ultra-low-latency connectivity suitable for industrial automation [8], [10], [11], [12], [13], [27], [36]. Cloud-native core functions support orchestration and service management, while the security layer enforces trust and cybersecurity policies. Multi-factory orchestration enables centralized management of geographically distributed industrial facilities.

The architecture provides enhanced scalability, reduced latency, improved resilience, and stronger cybersecurity compared with conventional industrial communication systems.

Advanced PKI Trust Management Framework:

Trust establishment is a critical requirement for Industrial IoT deployments because every connected device must be securely authenticated before joining the production network [22], [23], [24], [25], [26]. The proposed PKI framework supports secure onboarding, authentication, certificate lifecycle management, and zero-touch provisioning.

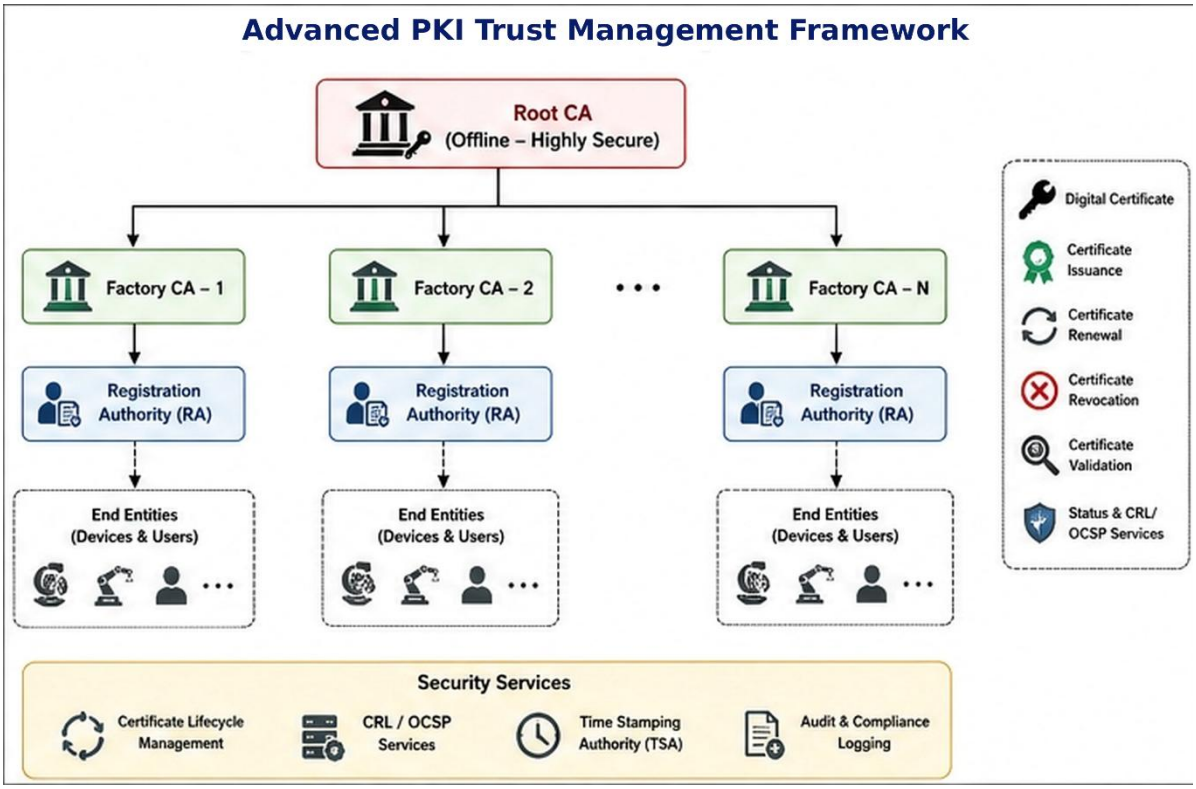


Figure (2): Advanced PKI Trust Management Framework.

The framework above consists of:

- Root Certificate Authority.
- Factory-Level Certificate Authorities.
- Registration Authorities.
- Certificate Lifecycle Services.
- Audit and Compliance Services.

Every industrial device receives a unique digital identity represented by an X.509 digital certificate to enable secure authentication and lifecycle management [22], [24], [25]. Secure onboarding begins with hardware-based identity verification followed by certificate issuance and network registration.

Table (2): Security Requirements and Implementation Mechanisms

Security Requirement	Description	Implementation Mechanism
Authentication	Verify device identity	X.509 Certificates
Authorization	Access control	RBAC + ABAC
Confidentiality	Protect data privacy	TLS 1.3 / IPSec
Integrity	Prevent tampering	Digital Signatures
Availability	Continuous operation	Redundancy & Failover
Non-Repudiation	Action traceability	PKI Audit Logs
Accountability	Compliance support	Security Monitoring
Trust Management	Device lifecycle security	Advanced PKI

The framework ensures confidentiality, integrity, availability, accountability, and non-repudiation while supporting large-scale industrial deployments.

Dynamic Network Slicing and AI-Driven Security:

Industrial applications exhibit diverse communication requirements that cannot be efficiently supported through a single network configuration; therefore, network slicing enables differentiated QoS provisioning for industrial services [8], [13], [14], [27], [28], [36], [37]. The proposed architecture employs dynamic network slicing to support differentiated service requirements.

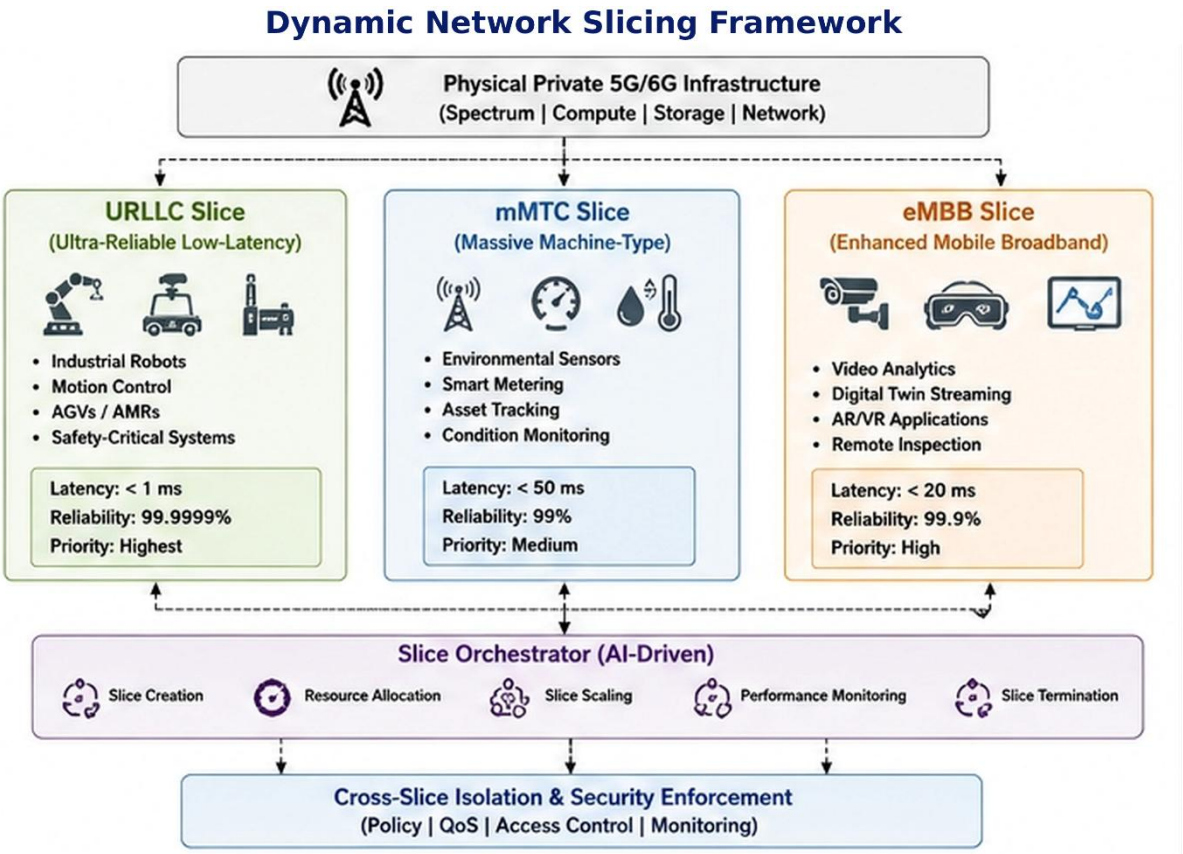


Figure (3): Dynamic Network Slicing Framework.

Three slice categories are defined:

- URLLC for robotics and motion control.
- mMTC for sensor networks and monitoring.
- eMBB for machine vision and digital twins.

Table (3): Industrial Network Slice Characteristics

Parameter	URLLC Slice	mMTC Slice	eMBB Slice
Main Applications	Robots, Motion Control	Sensors, Monitoring	Video Analytics
Latency	< 1 ms	< 50 ms	< 20 ms
Reliability	> 99.9999%	> 99%	> 99.9%
Device Density	Medium	Very High	Medium
Throughput	Medium	Low	Very High
Security Level	Critical	High	High
Priority	Highest	Medium	High

To enhance cybersecurity, the proposed architecture incorporates a federated learning-based GNN-GRU security engine capable of distributed threat detection while preserving local data privacy [29], [30], [31].

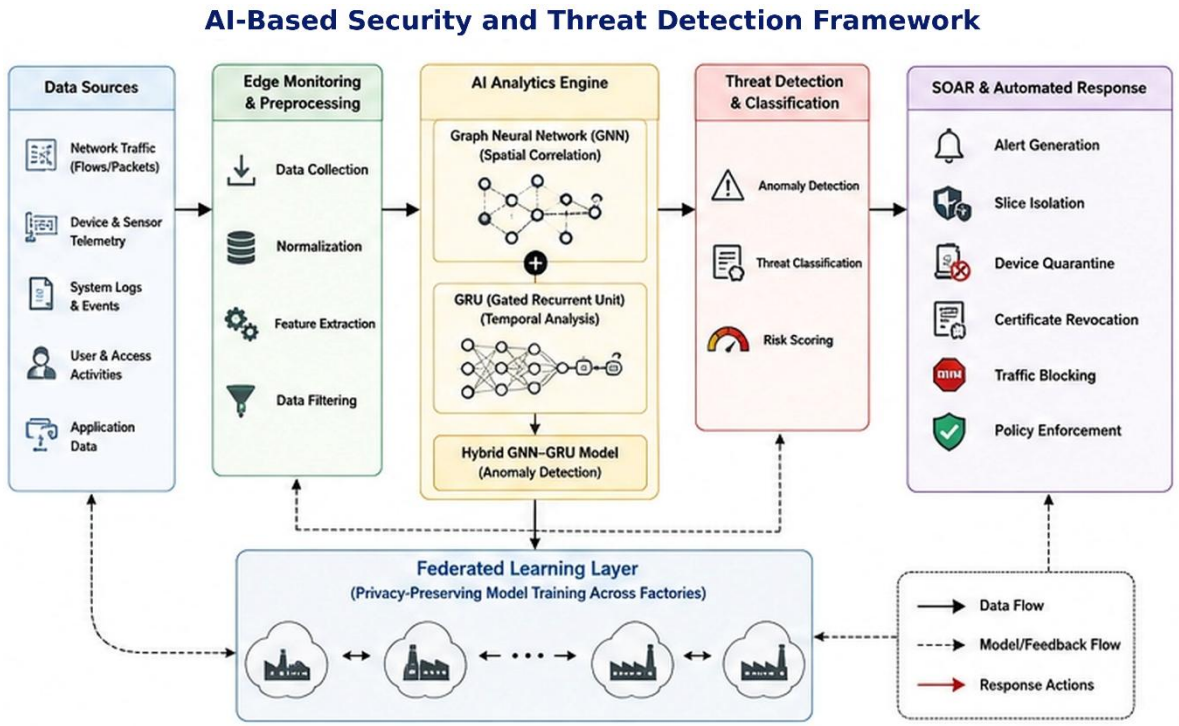


Figure (4): AI-Based Security and Threat Detection Framework.

The security engine continuously analyzes:

- Network traffic.
- Authentication events.
- Device behavior.
- Slice activities.

Threat intelligence is shared securely among participating factories, enabling coordinated defense against cyber threats.

Materials and Methods:

A simulation-based evaluation methodology was adopted using NS-3, UERANSIM, and OMNeT++ to evaluate networking performance under realistic industrial scenarios [32], [33], [34].

The experimental environment included:

- 15 factories.
- 1.5 million industrial devices.
- Three network slices.
- Federated learning-based security analytics.

Table (4): Simulation Parameters and Experimental Setup

Parameter	Value
Simulation Platform	NS-3, UERANSIM, OMNeT++
Simulation Duration	3600 seconds
Number of Factories	15
Devices per Factory	100,000
Total Devices	1,500,000
Network Slices	3
Edge Nodes per Factory	10
AI Model	Hybrid GNN-GRU
Security Model	PKI + Federated Learning
Attack Scenarios	DDoS, Spoofing, APT, Insider Threat
Traffic Types	URLLC, mMTC, eMBB

Performance was evaluated using:

- End-to-end latency.
- Throughput.
- Slice isolation accuracy.

- Threat detection rate.
- Scalability metrics.

Multiple cyberattack scenarios, including DDoS attacks, spoofing, insider threats, and advanced persistent threats (APTs), were implemented following recognized enterprise attack models [31], [35].

Materials and Methods:

The proposed architecture demonstrated substantial performance improvements compared with conventional industrial networking approaches.

Table (5): Performance Evaluation Results

Metric	Conventional Industrial Network	Conventional Private 5G	Proposed Framework
URLLC Latency	5.8 ms	1.8 ms	0.72 ms
mMTC Latency	12.1 ms	8.4 ms	3.1 ms
eMBB Latency	18.7 ms	12.6 ms	5.4 ms
Throughput	450 Mbps	980 Mbps	1.85 Gbps
Threat Detection Rate	81.2%	89.4%	97.2%
False Positive Rate	8.4%	4.7%	1.8%
Slice Isolation Accuracy	91.6%	93.8%	99.7%
Scalability	Medium	High	Very High

Key findings include:

- URLLC latency reduced to 0.72 ms.
- Throughput increased to 1.85 Gbps.
- Threat detection accuracy reached 97.2%.
- False positive rate reduced to 1.8%.
- Slice isolation accuracy improved to 99.7%.

These results demonstrate that integrating edge intelligence, network slicing, advanced PKI, and AI-driven security into a unified architecture substantially improves industrial communication performance and cyber resilience [13], [16], [27], [29], [30].

The multi-factory orchestration framework maintained consistent performance across geographically distributed industrial sites while supporting centralized policy enforcement and resource optimization.

Conclusion:

This paper presented a secure and scalable Industrial IoT architecture integrating Private 5G/6G networking, dynamic network slicing, edge intelligence, advanced PKI, and AI-driven cybersecurity for multi-factory environments [8], [13], [16], [22], [29], [30]. The proposed framework addresses critical challenges related to scalability, trust management, latency, and cybersecurity while providing a future-ready foundation for Industry 4.0 and Industry 5.0 deployments.

Simulation-based evaluation demonstrated significant improvements in communication performance, security effectiveness, and operational scalability. The integration of federated learning and GNN-GRU analytics further enhanced cyber resilience while preserving data privacy.

Future research will investigate quantum-safe cryptography, blockchain-based trust management, AI-native 6G networking, and real-world industrial pilot deployments.

References:

1. L. Da Xu, W. He, and S. Li, “Internet of Things in industries: A survey,” IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233–2243, 2014.
2. K. Schwab, The Fourth Industrial Revolution. Geneva, Switzerland: World Economic Forum, 2016.
3. S. Yin, O. Kaynak, and X. Li, “Industrial big data and intelligent manufacturing,” IEEE Transactions on Industrial Electronics, vol. 65, no. 8, pp. 6762–6765, 2018.
4. S. Wan, J. Lu, P. Fan, K. B. Letaief, and X. Cao, “Toward big data processing in IoT: Path planning and resource management,” IEEE Internet of Things Journal, vol. 7, no. 7, pp. 5995–6009, 2020.
5. European Commission, “Industry 5.0: Towards a sustainable, human-centric and resilient European industry,” Brussels, Belgium, 2021.
6. M. Wollschlaeger, T. Sauter, and J. Jasperneite, “The future of industrial communication,” IEEE Industrial Electronics Magazine, vol. 11, no. 1, pp. 17–27, 2017.
7. A. Mahmood, E. Sisinni, L. Guntupalli, R. Rondon, S. A. Hassan, and M. Gidlund, “Scalability analysis of industrial IoT networks,” IEEE Access, vol. 6, pp. 71562–71573, 2018.
8. 3GPP TS 23.501, “System architecture for the 5G system (5GS),” Release 18, 2024.
9. A. Aijaz and M. Sooriyabandara, “The tactile internet for industries: A review,” Proceedings of the IEEE, vol. 107, no. 2, pp. 414–435, 2019.

10. K. David and H. Berndt, “6G vision and requirements,” IEEE Vehicular Technology Magazine, vol. 13, no. 3, pp. 72–80, 2018.
11. M. Series, “IMT Vision – Framework and overall objectives of the future development of IMT for 2030 and beyond,” International Telecommunication Union (ITU), Geneva, Switzerland, 2023.
12. NGMN Alliance, “6G Position Statement: An Operator View,” Frankfurt, Germany, 2023.
13. Y. Liu, J. Li, and X. Wang, “Network slicing for industrial applications in 5G and beyond,” IEEE Access, vol. 12, pp. 14531–14549, 2024.
14. X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, “Network slicing in 5G: Survey and challenges,” IEEE Communications Magazine, vol. 55, no. 5, pp. 94–100, 2017.
15. N. Alliance, “Private 5G for industrial automation,” NGMN White Paper, 2024.
16. F. Restuccia and T. Melodia, “Deep learning at the edge for industrial IoT,” IEEE Communications Surveys & Tutorials, vol. 24, no. 4, pp. 2310–2345, 2022.
17. W. Shi and S. Dustdar, “The promise of edge computing,” Computer, vol. 49, no. 5, pp. 78–81, 2016.
18. P. Porambage, M. Liyanage, A. Braeken, C. Schmitt, and A. Gurtov, “The quest for privacy in the Internet of Things,” IEEE Cloud Computing, vol. 3, no. 2, pp. 36–45, 2016.
19. ETSI GS NFV 002, “Network Functions Virtualisation (NFV): Architectural Framework,” ETSI, Sophia Antipolis, France.
20. N. McKeown et al., “OpenFlow: Enabling innovation in campus networks,” ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69–74, 2008.
21. M. Satyanarayanan, “The emergence of edge computing,” Computer, vol. 50, no. 1, pp. 30–39, 2017.
22. C. Adams and S. Lloyd, Understanding PKI: Concepts, Standards, and Deployment Considerations, 2nd ed. Boston, MA, USA: Addison-Wesley, 2003.
23. NIST, “Zero Trust Architecture,” NIST Special Publication 800-207, Gaithersburg, MD, USA, 2020. [24] R. Housley, W. Ford, W. Polk, and D. Solo, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile,” IETF RFC 5280.
24. ENISA, “Good Practices for Security of IoT,” European Union Agency for Cybersecurity, 2020. [26] GSMA, “IoT SAFE: IoT SIM Applet For Secure End-to-End Communication,” GSMA White Paper, 2022.
25. H. Zhang, N. Liu, X. Chu, K. Long, A. Aghvami, and V. C. M. Leung, “Network slicing based 5G and future mobile networks,” IEEE Wireless Communications, vol. 24, no. 5, pp. 86–92, 2017.
26. M. Condoluci and T. Mahmoodi, “Softwarization and virtualization in 5G mobile networks,” IEEE Communications Magazine, vol. 53, no. 6, pp. 26–32, 2015.
27. A. Ferrag, L. Maglaras, H. Janicke, J. Jiang, and M. Shu, “Federated learning for cybersecurity in industrial IoT,” Future Generation Computer Systems, vol. 148, pp. 176–193, 2025.
28. Z. Zhao, Y. Liu, X. Wang, and K. Long, “AI-driven network management in 6G systems,” IEEE Network, vol. 38, no. 2, pp. 64–72, 2025.
29. W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, “Malware traffic classification using convolutional neural networks,” IEEE Access, vol. 5, pp. 1776–1787, 2017.
30. G. F. Riley and T. R. Henderson, The NS-3 Network Simulator. New York, NY, USA: ACM Press. UERANSIM Project Documentation, “Open-source 5G SA UE and gNodeB simulator,” 2025.
31. A. Varga and R. Hornig, “An overview of the OMNeT++ simulation environment,” Proc. Simutools, 2008.
32. MITRE Corporation, “MITRE ATT&CK Framework for Enterprise,” 2025.
33. P. Popovski et al., “Wireless access for ultra-reliable low-latency communication,” IEEE Network, vol. 35, no. 4, pp. 22–28, 2021.
34. S. K. Sharma and X. Wang, “Toward massive machine-type communications in 5G and beyond,” IEEE Communications Magazine, vol. 57, no. 9, pp. 86–91, 2019.
35. Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, “A survey on mobile edge computing,” IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2322–2358, 2017.
36. NIST, “Post-Quantum Cryptography Standardization,” National Institute of Standards and Technology, 2024.
37. S. R. Pokhrel and J. Choi, “Federated learning with blockchain for industrial systems,” IEEE Transactions on Industrial Informatics, vol. 20, no. 3, pp. 2145–2158, 2025.