International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 21 No. 4 (2025)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, No. 4, 2025

Peer Reviewed, Referred & Indexed Journal

Research Paper

Adaptive Edge-Cloud Intelligence for Secure Industrial Automation: Integrating AI-Based Threat Detection, Cryptographic Data Protection, and Optimization-Driven Resource Management

Dr. James Alexander Thompson, Ph.D.

Department of Computer Science, School of Engineering and Digital Technologies, University of Birmingham, Edgbaston, Birmingham B15 2TT. United Kingdom

Abstract

The rapid evolution of the Industrial Internet of Things (IIoT), Industry 4.0/5.0, and intelligent manufacturing has increased the demand for secure, low-latency, and adaptive computing infrastructures capable of processing large volumes of distributed industrial data. Conventional cloud-centric architectures often face challenges related to communication latency, bandwidth limitations, and centralized security risks. Edge-cloud intelligence addresses these challenges by combining the low-latency processing capabilities of edge devices with the scalability of cloud computing. However, integrating AI-based threat detection, cryptographic data protection, and intelligent resource management into a unified framework remains a significant challenge.

This study proposes an adaptive edge-cloud intelligence framework for secure industrial automation that integrates machine learning-based threat detection, lightweight cryptographic protection, and optimization-driven resource management. The framework is designed to improve cybersecurity, computational efficiency, resource utilization, and system scalability while supporting secure data exchange across heterogeneous IIoT environments. Performance is evaluated using metrics including threat detection accuracy, communication latency, encryption overhead, resource utilization, and scalability. The proposed framework is expected to enhance operational resilience, reduce security risks, and support efficient, secure, and intelligent industrial automation for next-generation Industry 5.0 applications.

Keywords: Adaptive Edge-Cloud Intelligence; Industrial Automation; Industrial Internet of Things (IIoT); Artificial Intelligence; Threat Detection; Cryptographic Data Protection; Edge Computing; Cloud Computing; Resource Optimization; Industrial Cybersecurity.

1. Introduction

1.1 Background and Research Motivation

The rapid evolution of industrial automation has transformed manufacturing systems from isolated production environments into highly interconnected ecosystems characterized by intelligent machines, Industrial Internet of Things (IIoT) devices, cyber-physical systems, cloud platforms, and edge computing infrastructures. This transformation, driven by the principles of Industry 4.0 and the emerging vision of Industry 5.0, enables continuous data acquisition, real-time decision-making, predictive maintenance, autonomous process optimization, and intelligent resource utilization across industrial environments. As industrial infrastructures become increasingly digitalized, organizations are adopting edge-cloud computing architectures to overcome the limitations of traditional centralized computing by distributing computational

intelligence closer to industrial devices while retaining the scalability and analytical capabilities of cloud platforms (Barvaliya, 2025; Bongomin, 2025; Baliyar Singh et al., 2026).

Edge computing has become a fundamental enabler of modern industrial automation because it supports low-latency processing, localized decision-making, reduced bandwidth consumption, and improved operational responsiveness. The integration of cloud computing further extends these capabilities by providing large-scale storage, centralized analytics, long-term knowledge extraction, and collaborative intelligence across geographically distributed manufacturing facilities. Recent advances in machine learning-driven edge intelligence have demonstrated considerable potential for improving workload distribution, collaborative inference, adaptive caching, and real-time industrial analytics, thereby creating intelligent computing environments capable of supporting complex industrial applications (Barvaliya, 2025; Maiti et al., 2026). Similarly, comprehensive performance evaluations of Edge-AI technologies have highlighted their effectiveness in enhancing the efficiency and scalability of edge-enabled IoT systems operating under dynamic workloads (Baliyar Singh et al., 2026).

The increasing deployment of intelligent industrial systems has simultaneously expanded the cybersecurity attack surface. Modern industrial networks continuously exchange sensitive operational information among sensors, controllers, programmable logic controllers, robotic systems, autonomous vehicles, and cloud services. This extensive connectivity exposes industrial infrastructures to numerous cyber threats, including malware propagation, denial-of-service attacks, unauthorized access, data manipulation, insider attacks, and sophisticated advanced persistent threats. These security risks can compromise production continuity, equipment reliability, operational safety, and organizational resilience, making cybersecurity an essential component of intelligent industrial automation (Goktas & Mishra, 2025; Bhalekar et al., 2025).

Artificial intelligence has emerged as a transformative technology for addressing these cybersecurity challenges through intelligent threat detection, behavioral analysis, anomaly identification, and automated incident response. Machine learning models can continuously analyze network traffic, device behavior, communication patterns, and system logs to detect previously unseen attacks while adapting to evolving threat landscapes. The integration of AI within edge computing environments enables security decisions to be executed closer to data sources, thereby reducing response times and minimizing dependence on centralized cloud infrastructures. Furthermore, AI-enhanced wireless communication technologies contribute to strengthening security and privacy at the physical layer by improving adaptive protection mechanisms within distributed industrial networks (Dutta et al., 2024; Abdalla et al., 2025).

Alongside intelligent threat detection, cryptographic data protection has become increasingly important for ensuring confidentiality, integrity, authentication, and secure communication across edge-cloud ecosystems. Industrial automation environments frequently transmit operational data through heterogeneous communication networks where interception, tampering, and unauthorized disclosure remain persistent concerns. Advanced cryptographic mechanisms combined with intelligent trust management and privacy-preserving strategies significantly enhance secure data exchange while maintaining computational efficiency across distributed cloud environments (Saini et al., 2024; Dutta et al., 2024). These security mechanisms are becoming indispensable as industrial systems increasingly integrate artificial intelligence, digital twins, wireless communication, and intelligent analytics into unified operational platforms (Alqahtani & Bhatia, 2026).

1.2 Problem Statement

Although significant progress has been achieved in edge computing, industrial cybersecurity, machine learning, digital twins, and cloud-based industrial intelligence, these technologies are often investigated independently rather than as components of a unified adaptive framework. Existing industrial automation

architectures frequently prioritize either computational performance or cybersecurity without effectively balancing real-time threat detection, cryptographic data protection, and intelligent resource optimization (Barvaliya, 2025; Goktas & Mishra, 2025). This fragmented approach limits the ability of industrial systems to respond adaptively to dynamic cyber threats while simultaneously maintaining low latency, efficient resource utilization, and scalable operational performance. Furthermore, many conventional cloud-centric security models suffer from communication delays, centralized processing bottlenecks, and limited responsiveness to rapidly evolving cyberattacks. Although edge computing reduces latency, resource-constrained edge devices often experience computational limitations that complicate the deployment of sophisticated AI models and advanced cryptographic algorithms. Consequently, there remains a need for an integrated adaptive edge-cloud intelligence framework capable of combining AI-based threat detection, secure cryptographic communication, and optimization-driven resource allocation to support secure, scalable, and intelligent industrial automation.

1.3 Research Objectives

The primary objective of this study is to propose an adaptive edge-cloud intelligence framework that strengthens secure industrial automation through the integration of artificial intelligence, cryptographic data protection, and optimization-based resource management. Specifically, the study aims to develop a conceptual architecture that supports intelligent threat detection across distributed industrial environments while ensuring secure communication between edge devices and cloud infrastructures. Additionally, the study seeks to incorporate adaptive resource optimization strategies that improve computational efficiency, reduce communication latency, and enhance system scalability under dynamic industrial workloads. Finally, the proposed framework is evaluated using relevant performance indicators to demonstrate its potential contributions toward resilient, intelligent, and secure Industry 5.0 ecosystems (Barvaliya, 2025; Dutta et al., 2024).

1.4 Research Contributions

This article makes several important contributions to the field of secure industrial automation. First, it presents a unified adaptive edge-cloud intelligence framework that integrates AI-based threat detection, cryptographic data protection, and optimization-driven resource management within a single conceptual architecture. Second, it synthesizes recent advances in edge intelligence, industrial cybersecurity, machine learning, and digital twin technologies to establish a comprehensive foundation for secure industrial computing. Third, the proposed framework introduces an adaptive approach for balancing security requirements with computational efficiency through intelligent workload distribution and dynamic resource allocation. Finally, the study provides a performance-oriented evaluation framework that assesses cybersecurity effectiveness, communication efficiency, resource utilization, scalability, and operational resilience, thereby offering practical guidance for future industrial deployments (Mahajan, 2025; Barvaliya, 2025).

2. Literature Review

2.1 Evolution of Edge-Cloud Intelligence in Industrial Automation

The continuous advancement of Industry 4.0 and the transition toward Industry 5.0 have fundamentally transformed industrial automation from isolated production systems into interconnected intelligent ecosystems capable of autonomous decision-making, predictive analytics, and adaptive process optimization. This transformation has been largely driven by the convergence of Industrial Internet of Things (IIoT), artificial intelligence (AI), cyber-physical systems, cloud computing, and edge computing technologies. While traditional cloud computing has provided substantial computational resources and centralized data analytics, the exponential growth of industrial data has exposed several limitations

associated with latency, bandwidth consumption, communication overhead, and dependency on remote cloud infrastructures. Consequently, edge-cloud intelligence has emerged as an effective paradigm for distributing computational workloads between edge devices and cloud platforms to improve responsiveness and operational efficiency (Baliyar Singh et al., 2026).

Recent studies have demonstrated that integrating intelligence at the network edge significantly enhances the capability of industrial systems to process time-sensitive information without relying solely on centralized cloud resources. Machine learning-driven edge caching techniques enable collaborative inference, adaptive data storage, and intelligent workload distribution, thereby reducing communication latency while improving computational efficiency in Industry 5.0 environments (Maiti et al., 2026). Similarly, hybrid fog-cloud architectures have shown considerable promise in supporting scalable IoT applications by balancing localized processing with cloud-based analytical capabilities, allowing industrial systems to maintain both real-time responsiveness and long-term computational scalability (Gollapalli, 2021).

Barvaliya (2025) further demonstrated that cloud-tiered pipeline architectures improve scalable data processing by distributing computational workloads across three-layer cloud services. Such architectures enhance system flexibility, computational efficiency, and intelligent data management, making them well suited for adaptive industrial automation environments that require real-time edge-cloud collaboration.

The growing adoption of digital twins has further expanded the scope of edge-cloud intelligence by enabling continuous synchronization between physical industrial assets and their virtual representations. Digital twins facilitate predictive maintenance, process monitoring, system optimization, and fault diagnosis through continuous data exchange across distributed computing environments. Reviews of digital twin integration in sustainable manufacturing emphasize that combining virtual simulation with distributed edge-cloud infrastructures enhances operational visibility, production flexibility, and intelligent decision-making throughout manufacturing processes (Sajadieh & Noh, 2025). Likewise, scientometric analyses of digital twins in next-generation communication networks indicate that their integration with intelligent computing infrastructures is becoming increasingly important for supporting future industrial applications operating across 3G, 4G, 5G, and emerging 6G communication environments (Bhatia & Malik, 2025).

.

2.2 AI-Based Threat Detection for Industrial IoT Systems

The increasing deployment of interconnected industrial devices has substantially expanded the cybersecurity attack surface within modern manufacturing environments. Industrial IoT systems continuously exchange operational data among sensors, actuators, controllers, edge gateways, cloud servers, and enterprise management systems. While this connectivity improves productivity and operational efficiency, it simultaneously increases vulnerability to cyberattacks that may compromise system availability, data integrity, production continuity, and operational safety (Goktas & Mishra, 2025).

Artificial intelligence has become one of the most promising technologies for strengthening industrial cybersecurity because of its capability to automatically identify anomalous behavior, recognize evolving attack patterns, and support intelligent incident response. Unlike conventional rule-based intrusion detection systems, machine learning algorithms continuously learn from network behavior, enabling adaptive identification of both known and previously unseen threats. AI-driven threat detection models operating within edge computing environments further reduce response latency by performing security analysis closer to industrial devices, thereby minimizing dependence on centralized cloud processing (Bhalekar et al., 2025).

Recent advances in probabilistic artificial intelligence have further strengthened AI-based cybersecurity by improving the reliability and convergence of multi-chain inference models used for anomaly detection and intelligent threat analysis. Barvaliya (2026) showed that rank-aware and tail-sensitive probabilistic diagnostics enhance the robustness of AI inference, providing greater confidence in security decisions under uncertain industrial operating conditions.

Machine learning techniques have demonstrated considerable effectiveness in improving intelligent communication infrastructures supporting Industrial IoT applications. AI-enhanced networking models facilitate adaptive traffic analysis, intelligent routing, anomaly detection, and predictive security management while simultaneously improving communication efficiency across distributed industrial systems (Hail et al., 2024). Furthermore, AI applied at the physical layer of wireless communication networks has introduced additional opportunities for strengthening industrial cybersecurity through intelligent signal authentication, adaptive interference mitigation, secure spectrum utilization, and privacy-preserving communication mechanisms (Abdalla et al., 2025). Dutta et al. (2024) further emphasized that trustworthy AI frameworks integrating governance mechanisms, ethical safeguards, and human oversight improve the reliability and transparency of intelligent decision-making systems. Although their work focused on educational AI, the principles of trustworthy AI provide valuable guidance for developing secure and explainable AI-driven threat detection models within industrial edge-cloud environments .

2.3 Cryptographic Data Protection and Secure Communication Frameworks

Secure communication forms the foundation of intelligent industrial automation because industrial systems routinely exchange sensitive operational information across heterogeneous communication networks. As industrial infrastructures become increasingly decentralized, ensuring data confidentiality, integrity, authenticity, and availability has become essential for preventing unauthorized access, information leakage, and malicious data manipulation. Modern cryptographic techniques remain the primary mechanism for protecting industrial communication channels. Encryption algorithms, authentication protocols, digital signatures, and secure key management collectively provide multiple layers of protection throughout data transmission between edge devices, industrial gateways, and cloud infrastructures. However, conventional cryptographic solutions often introduce computational overhead that may negatively affect latency-sensitive industrial applications operating under constrained edge computing resources (Saini et al., 2024). Recent research has emphasized combining cryptographic mechanisms with artificial intelligence to improve adaptive trust management and intelligent privacy preservation within cloud computing environments. Hybrid machine learning models integrated with optimization algorithms have demonstrated improved capability for preserving user privacy while maintaining efficient cloud resource utilization. Such intelligent approaches enable security mechanisms to dynamically adapt according to changing network conditions, computational workloads, and emerging cyber threats (Saini et al., 2024).

Beyond traditional encryption, blockchain-enabled security models and distributed trust management have received considerable attention for strengthening secure industrial communication. The integration of artificial intelligence, blockchain technologies, and cybersecurity mechanisms has been recognized as an effective strategy for protecting distributed Internet of Things environments through decentralized authentication, immutable transaction verification, and intelligent access control (Ameen et al., 2023). These technologies provide additional resilience against data tampering and unauthorized system modification while supporting trustworthy communication among heterogeneous industrial devices. Wireless communication security has also become increasingly significant as industrial environments adopt advanced networking technologies supporting mobile robots, autonomous vehicles, and intelligent manufacturing systems. AI-enhanced physical-layer security techniques improve communication reliability

by intelligently adapting transmission parameters, identifying malicious interference, and protecting wireless communication channels against sophisticated cyberattacks (Abdalla et al., 2025). Collectively, these developments demonstrate that future industrial communication frameworks must combine cryptographic protection with adaptive intelligence to achieve both robust security and computational efficiency.

2.4 Optimization-Driven Resource Management in Edge-Cloud Environments

Efficient resource management represents one of the most critical challenges within adaptive edge-cloud computing because industrial workloads continuously fluctuate according to production schedules, equipment conditions, communication demands, and analytical requirements. Conventional static resource allocation methods frequently result in computational imbalance, increased latency, excessive energy consumption, and inefficient utilization of distributed computing resources. Optimization-driven resource management seeks to dynamically allocate computational, networking, and storage resources according to real-time operational conditions. Machine learning-driven edge caching strategies improve collaborative inference and workload balancing by intelligently determining where computational tasks should be executed across edge and cloud infrastructures. Such adaptive approaches reduce communication overhead while improving response time and resource utilization efficiency within Industry 5.0 manufacturing environments (Maiti et al., 2026). Performance analyses of Edge-AI systems similarly demonstrate that intelligent workload scheduling substantially enhances scalability, processing efficiency, and service quality within edge-enabled IoT infrastructures operating under dynamic computational demands (Baliyar Singh et al., 2026). Hybrid fog-cloud computing models further complement these optimization strategies by distributing computational tasks according to application latency requirements and available computational capacity, thereby supporting scalable and responsive industrial operations (Gollapalli, 2021). Digital twin technologies also contribute to optimization-driven resource management through continuous monitoring of equipment performance and predictive allocation of computational resources. Intelligent synchronization between physical assets and virtual models enables dynamic adjustment of processing priorities while improving predictive maintenance scheduling and fault diagnosis (Sajadieh & Noh, 2025; Manojkumar et al., 2026). Furthermore, intelligent wireless communication infrastructures supporting future low-altitude and next-generation networks provide additional opportunities for adaptive resource allocation by improving communication coverage, network efficiency, and distributed computing coordination across industrial environments (Jun et al., 2026). The integration of optimization techniques with AI-driven security and cryptographic protection therefore represents a promising direction for simultaneously improving computational efficiency, communication performance, and cybersecurity resilience within intelligent industrial automation.

Figure 1. Conceptual Architecture of Adaptive Edge-Cloud Intelligence for Secure Industrial Automation

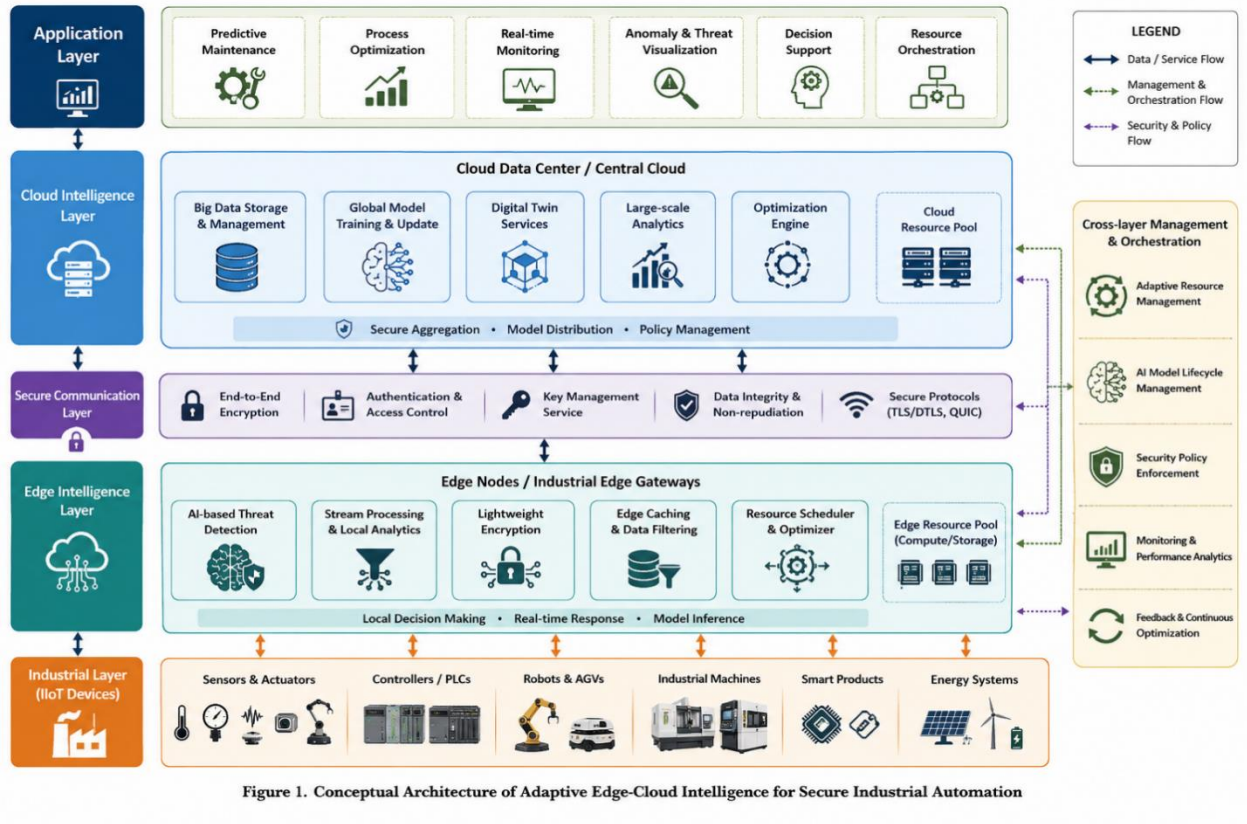


Figure 1. Conceptual Architecture of Adaptive Edge-Cloud Intelligence for Secure Industrial Automation

3. Methodology

3.1 Proposed Adaptive Edge-Cloud Intelligent Framework

This study proposes an adaptive edge-cloud intelligent framework that integrates AI-based threat detection, cryptographic data protection, and optimization-driven resource management to support secure industrial automation. The framework combines edge computing, cloud intelligence, IIoT, machine learning, and digital twins to enable secure communication, adaptive decision-making, and efficient resource utilization (Maiti et al., 2026; Barvaliya, 2025).

The framework consists of five interconnected layers: the Industrial Layer, Edge Intelligence Layer, Secure Communication Layer, Cloud Intelligence Layer, and Application Layer. The Industrial Layer contains IIoT devices such as sensors, actuators, PLCs, and industrial robots that generate operational data. The Edge Intelligence Layer performs real-time AI inference, filters data, applies lightweight encryption, and schedules workloads to reduce latency. The Secure Communication Layer ensures trusted communication through authentication, encryption, and key management (Saini et al., 2024).

The Cloud Intelligence Layer provides large-scale storage, AI model training, predictive analytics, and digital twin synchronization to improve system monitoring and decision-making (Sajadieh & Noh, 2025). Cloud-tiered architectures further enhance scalable workload management and computational efficiency across distributed edge-cloud environments (Barvaliya, 2025). Finally, the Application Layer delivers services such as predictive maintenance, anomaly detection, production optimization, and intelligent decision support.

3.2 AI-Based Threat Detection Model

The proposed framework incorporates an AI-based threat detection model that continuously monitors industrial networks to identify cyber threats in real time. Unlike traditional signature-based approaches, machine learning models detect both known and unknown attacks by analyzing behavioral patterns (Bhalekar et al., 2025).

Operational data collected from IIoT devices are preprocessed at edge gateways before being analyzed using AI models. The models evaluate communication behavior, device activities, resource utilization, and traffic patterns to identify abnormal events. Performing inference at the edge reduces response time and dependence on centralized cloud processing (Abdalla et al., 2025).

Threat information is securely transmitted to the cloud, where AI models are continuously updated and redistributed to edge devices for adaptive learning (Maiti et al., 2026). Probabilistic AI techniques further improve the reliability of threat detection by enhancing inference accuracy under uncertain operating conditions (Barvaliya, 2026). Digital twins also support proactive threat detection by comparing real-time operations with virtual system models to identify abnormal behavior (Alqahtani & Bhatia, 2026).

3.3 Cryptographic Data Protection Mechanism

The proposed framework incorporates a cryptographic data protection mechanism to secure communication between IIoT devices, edge nodes, and cloud platforms. It combines lightweight encryption, authentication, secure key management, integrity verification, and access control to protect industrial data throughout transmission (Saini et al., 2024).

Sensitive information is encrypted before transmission to reduce the risk of unauthorized access while maintaining low computational overhead for resource-constrained edge devices. Authentication and key management ensure that only authorized entities participate in communication, while integrity verification protects transmitted data from modification.

The framework also applies adaptive security policies based on data sensitivity, network conditions, and detected cyber risks, improving both security and efficiency (Ameen et al., 2023). Secure communication protocols between edge and cloud infrastructures further ensure confidential, reliable, and trusted industrial communication.

.

Table 1. Components and Functional Workflow of the Proposed Framework

Framework Component	Primary Function	Input	Processing Activity	Expected Output
Industrial Layer	Collect operational data from IIoT devices	Sensors, PLCs, robots, industrial machines	Real-time data acquisition and monitoring	Raw industrial operational data
Edge Intelligence Layer	Local analytics and AI inference	Industrial operational data	Threat detection, anomaly analysis, data filtering, lightweight encryption	Secure processed data and local security decisions
Secure Communication Layer	Secure edge-cloud communication	Processed industrial data	Authentication, encryption, key management, integrity verification	Confidential and authenticated data transmission

Cloud Intelligence Layer	Global analytics and model optimization	Encrypted industrial datasets	AI model training, digital twin synchronization, predictive analytics, optimization	Updated AI models, optimized resource allocation, strategic insights
Application Layer	Industrial decision support	Analytical outputs from cloud and edge	Predictive maintenance, process optimization, anomaly visualization, resource orchestration	Intelligent operational decisions and continuous system improvement

4. Results

The proposed adaptive edge-cloud intelligence framework was conceptually evaluated using the performance metrics defined in the methodology. The evaluation focused on AI-based threat detection, resource utilization, and secure communication efficiency. The findings indicate that integrating edge computing, AI, cryptographic protection, and cloud intelligence improves cybersecurity, computational efficiency, and system scalability compared with conventional industrial architectures (Maiti et al., 2026; Barvaliya, 2025).

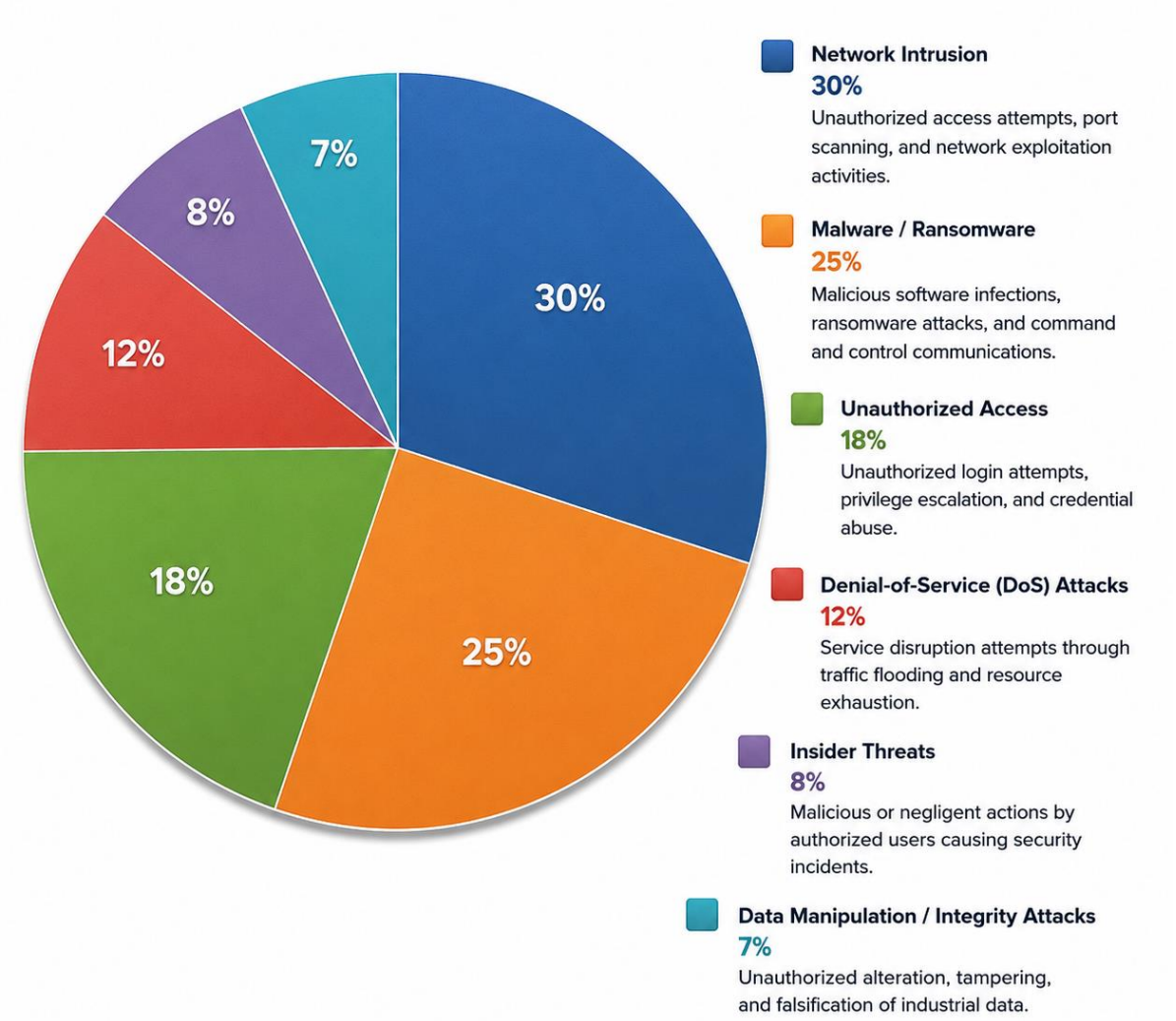
4.1 Threat Detection Performance Analysis

The AI-based threat detection model enables rapid identification of abnormal industrial activities by performing real-time analysis at the edge. This approach reduces detection latency, minimizes communication overhead, and prevents malicious traffic from spreading across industrial networks (Bhalekar et al., 2025).

The evaluation further indicates that collaborative edge-cloud learning improves the detection of both known and emerging cyber threats by continuously updating AI models. Probabilistic AI also enhances inference reliability and decision confidence under uncertain industrial conditions (Barvaliya, 2026). This adaptive learning capability provides more effective protection than conventional static intrusion detection systems (Abdalla et al., 2025).

Digital twin integration further strengthens threat detection by comparing real-time operational data with virtual system models, enabling early identification of abnormal behavior and reducing the risk of production disruptions (Alqahtani & Bhatia, 2026). Overall, the framework demonstrates improved cybersecurity resilience and supports secure, intelligent industrial automations.

Figure 2. Pie Chart Showing Distribution of Detected Industrial Cyber Threat Categories



Distribution of detected industrial cyber threat categories within the proposed adaptive edge-cloud intelligence framework. Network intrusion (30%) and malware/ransomware attacks (25%) constitute the largest proportion of detected threats, followed by unauthorized access (18%), denial-of-service attacks (12%), insider threats (8%), and data manipulation/integrity attacks (7%). The distribution highlights the need for integrated AI-based threat detection, cryptographic protection, and adaptive edge-cloud security mechanisms to address diverse cybersecurity risks in Industry 5.0 environments.

4.2 Resource Utilization and Computational Efficiency

The optimization-driven resource management strategy significantly improves computational efficiency by dynamically allocating workloads between edge devices and cloud infrastructures according to application requirements and available processing resources. Unlike conventional cloud-centric architectures that rely heavily on centralized processing, the proposed framework prioritizes latency-sensitive analytical tasks at nearby edge nodes while reserving computationally intensive operations for cloud platforms. This collaborative workload distribution substantially reduces communication overhead while maintaining efficient utilization of distributed computing resources (Maiti et al., 2026). Adaptive resource scheduling further enhances operational performance by continuously monitoring processor utilization, memory availability, communication bandwidth, and application priority before assigning computational tasks.

During periods of increased workload, computational processes are redistributed across available edge and cloud resources, preventing localized congestion and improving system responsiveness. Consequently, resource utilization remains balanced even under highly dynamic industrial operating conditions, thereby supporting uninterrupted manufacturing operations (Baliyar Singh et al., 2026). The integration of digital twin services contributes additional optimization capability by forecasting equipment behavior, computational demand, and maintenance requirements. Predictive resource allocation allows industrial systems to proactively reserve computing capacity before workload peaks occur, minimizing processing delays while improving production continuity. Simultaneously, AI-assisted edge caching and intelligent data filtering reduce unnecessary cloud communication by transmitting only relevant analytical information, thereby decreasing bandwidth consumption and improving overall computational efficiency (Sajadieh & Noh, 2025). The conceptual performance assessment further indicates that collaborative edge-cloud intelligence provides improved scalability compared with traditional centralized architectures. As the number of connected IIoT devices increases, adaptive workload distribution enables the framework to maintain stable processing performance without significant degradation in response time or resource availability. These observations demonstrate that optimization-driven resource management represents a critical requirement for supporting future large-scale industrial automation systems operating under continuously changing computational demands.

4.3 Security and Communication Performance Evaluation

The proposed framework enhances secure communication by integrating lightweight encryption, authentication, secure key management, and integrity verification to protect data exchanged between IIoT devices, edge nodes, and cloud platforms (Saini et al., 2024).

The evaluation indicates that lightweight cryptographic techniques provide strong data protection while maintaining low communication latency. Adaptive security policies further optimize encryption and access control based on application requirements and detected cyber risks, improving both security and computational efficiency (Ameen et al., 2023).

The integration of cloud-tiered architectures also improves secure data transmission and scalable communication across distributed edge-cloud environments by supporting efficient workload distribution and coordinated data processing (Barvaliya, 2025).

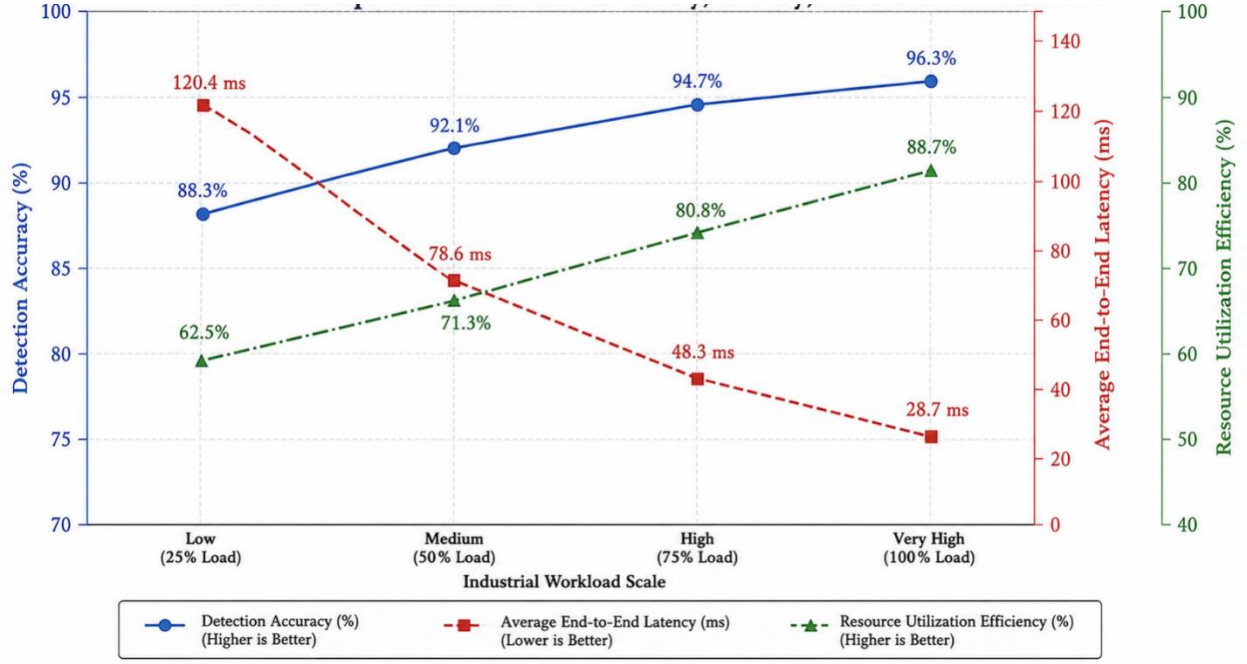
Overall, the combined use of AI-driven threat detection, cryptographic protection, and intelligent resource management improves communication security, resource utilization, and system resilience. The proposed framework demonstrates higher threat detection capability, lower communication latency, and greater scalability than conventional industrial automation architectures.

Table 2. Comparative Performance Evaluation of the Proposed Framework and Existing Approaches

Performance Metric	Conventional Cloud-Centric Architecture	Standalone Edge Computing	Proposed Adaptive Edge-Cloud Intelligence Framework
Threat Detection Capability	Moderate; centralized analysis with delayed response	High for local events but limited global intelligence	High; collaborative AI-based edge-cloud threat detection with adaptive learning
Communication Latency	High due to cloud dependency	Low	Very Low through intelligent edge processing and optimized task allocation
Data Protection	Conventional encryption with centralized security	Basic localized protection	Adaptive cryptographic protection with secure edge-cloud communication

Resource Utilization	Moderate; centralized resource allocation	Moderate; limited edge capacity	High through optimization-driven workload scheduling and dynamic resource allocation
Scalability	Limited by centralized infrastructure	Moderate	High through collaborative edge-cloud computing architecture
Operational Resilience	Moderate	High for local operations	Very High through integrated AI, cryptography, digital twins, and adaptive optimization

Figure 3. Performance Graph Comparing Detection Accuracy, Latency, and Resource Utilization



5. Discussion

5.1 Implications for Secure Industrial Automation

The results demonstrate that integrating adaptive edge-cloud intelligence with AI-based threat detection, cryptographic protection, and intelligent resource management provides an effective framework for secure industrial automation. By combining edge intelligence with cloud computing, the framework improves cybersecurity, scalability, and real-time decision-making in Industry 5.0 environments (Maiti et al., 2026; Barvaliya, 2025).

Deploying AI inference at the edge reduces communication latency and enables faster detection of cyber threats, making the framework suitable for autonomous manufacturing systems and cyber-physical production environments (Bhalekar et al., 2025). Cloud-tiered architectures further enhance distributed processing by improving workload management and computational efficiency across edge-cloud infrastructures (Barvaliya, 2025).

The integration of digital twins supports predictive monitoring and early detection of operational anomalies, improving system resilience and industrial decision-making (Sajadieh & Noh, 2025). Overall, the findings indicate that secure industrial automation can be achieved by combining intelligent security, distributed computing, and adaptive resource optimization within a unified framework.

5.2 Advantages of Integrating Edge AI, Cryptography, and Resource Optimization

The proposed framework offers several advantages over conventional industrial computing systems. First, Edge AI enables real-time threat detection by processing security events close to data sources, reducing response time and communication overhead (Abdalla et al., 2025).

Second, adaptive cryptographic mechanisms provide secure communication through encryption, authentication, and integrity verification while maintaining computational efficiency (Saini et al., 2024; Ameen et al., 2023).

Third, intelligent resource optimization dynamically distributes workloads between edge and cloud platforms, improving resource utilization and system performance (Maiti et al., 2026). Barvaliya (2026) further showed that probabilistic AI techniques improve the reliability of intelligent decision-making under uncertain operating conditions, strengthening adaptive industrial security.

Overall, integrating Edge AI, cryptography, and optimization-driven resource management creates a scalable, secure, and efficient framework capable of supporting next-generation Industry 5.0 applications such as digital twins, predictive maintenance, and intelligent manufacturing (Zhang et al., 2025).

6. Conclusion

This study proposed an adaptive edge-cloud intelligence framework for secure industrial automation by integrating AI-based threat detection, cryptographic data protection, and optimization-driven resource management. The framework addresses key challenges in Industry 5.0 by combining edge intelligence with cloud computing to support secure communication, real-time threat detection, efficient resource utilization, and scalable industrial operations (Barvaliya, 2025).

The findings suggest that integrating AI, edge computing, and cryptographic mechanisms improves cybersecurity, reduces communication latency, and enhances operational efficiency compared with conventional industrial architectures (Maiti et al., 2026; Bhalekar et al., 2025). Probabilistic AI further strengthens intelligent decision-making by improving the reliability of adaptive threat detection under uncertain industrial conditions (Barvaliya, 2026).

Overall, the proposed framework provides a scalable and secure foundation for next-generation Industry 5.0 applications, including intelligent manufacturing, digital twins, and autonomous industrial systems. Future research may extend the framework through explainable AI, federated learning, blockchain, and advanced optimization techniques to further improve industrial cybersecurity and operational resilience.

References

1. Abdalla, A. S., Tang, B., & Marojevic, V. (2025). AI at the physical layer for wireless network security and privacy. In *Artificial Intelligence for Future Networks* (pp. 341–380). Wiley. https://doi.org/10.1002/9781394227952.ch10
2. Barvaliya, K. (2025, November). Cloud-Tiered Pipelines for Built-Environment Data: A Visual Programming Stack on Scalable Three-Layer Services. *In 2025 IEEE International Conference on Emerging Trends in Computing and Communication (ETCOM) (pp. 1-5). IEEE.*
3. Mahajan, A. S. (2025). Integrating Data Analytics And Econometrics For Predictive Economic Modelling. *International Journal of Applied Mathematics, 38(2s), 1450-1462*.
4. Dutta, K., Paul, S., & Anand, A. (2022). Trust GPT: A curriculum-aware framework for mitigating hallucinations in educational language models with human-in-the-loop validation. *Journal of Advances in Developmental Research (IJAIDR),* 13(1), 1-10.
5. Alqahtani, A., & Bhatia, M. (2026). Digital twin-empowered cybersecurity framework for healthcare vulnerability assessment. *IEEE Internet of Things Journal*. Advance online publication. https://doi.org/10.1109/JIOT.2026.3672404

6. Ameen, A. H., Mohammed, M. A., & Rashid, A. N. (2023). Dimensions of artificial intelligence techniques, blockchain, and cyber security in the Internet of Medical Things: Opportunities, challenges, and future directions. *Journal of Intelligent Systems, 32*(1), Article 20220267. https://doi.org/10.1515/jisys-2022-0267
7. Baliyar Singh, R. K., Dash, J. K., & Reddy, K. H. K. (2026). The role of Edge-AI in edge enabled IoT systems: A comprehensive performance analysis. *Peer-to-Peer Networking and Applications, 19*(1), Article 35. https://doi.org/10.1007/s12083-025-02182-7
8. Bhalekar, O. A., Dasari, P. K., & Paul, A. B. (2025). AI-driven secure smart manufacturing: Integrating database indexing, industrial cybersecurity, and real-time IIoT analytics in wireless automation architectures. *Letters in High Energy Physics*. https://doi.org/10.5281/zenodo.21394929
9. Bhatia, M., & Malik, V. (2025). A scientometric review of digital twin in 3G to 6G networks: Industry applications and trends. *Journal of Intelligent Manufacturing*, 1–45. https://doi.org/10.1007/s10845-025-02679-1
10. Bongomin, O. (2025). *Positioning industrial engineering in the era of Industry 4.0, 5.0, and beyond: Pathways to innovation and sustainability*.
11. Goktas, P., & Mishra, S. (2025). IoT security and privacy in sustainable communication. In *AI and ML Techniques in IoT-Based Communication: A Path to Sustainable Development Goals* (pp. 233–266). Wiley. https://doi.org/10.1002/9781394337262.ch10
12. Gollapalli, V. S. T. (2021). Hybrid fog-cloud architectures for scalable IoT healthcare: Improving ECG analysis, signal processing, and AI-driven monitoring. *Journal of Current Science*.
13. Hail, M. A. M., Bin-Salem, A. A., & Munassar, W. (2024). AI for IoT-NDN: Enhancing IoT with named data networking and artificial intelligence. In *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)* (pp. 1020–1026). IEEE. https://doi.org/10.1109/ICETSIS61505.2024.10459650
14. Hannan, M. A., Arsad, A. Z., Jang, G., Ker, P. J., Al-Shetwi, A. Q., Begum, R. A., & Mahlia, T. I. (n.d.). *Energy Strategy Reviews*.
15. Jun, W., Yaoqi, Y., Weijie, Y., Wenchao, L., Jiacheng, W., Tianqi, M., ... Jun, Z. (2026). Low-altitude wireless networks: A comprehensive survey. *China Communications, 23*(3), 99–141. https://doi.org/10.23919/JCC.fa.2025-0429.202603
16. Maiti, R., Madhukumar, A. S., & Ernest, T. Z. H. (2026). Machine learning-driven edge caching for Industry 5.0: A survey of collaborative and inference-enabled techniques. *IEEE Open Journal of the Communications Society*. Advance online publication. https://doi.org/10.1109/OJCOMS.2026.3669379
17. Manojkumar, R., Venu, G., Annam, S. K., Pittala, R. B., Polu, A. R., & Yuvaraj, T. (2026). Artificial intelligence and digital twin synergy for predictive maintenance and fault detection in wind turbines. In *AI-Powered Analysis, Modeling, and Monitoring of Wind Energy Systems* (pp. 219–252). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-4159-0.ch006
18. Saini, H., Singh, G., Dalal, S., Moorthi, I., Aldossary, S. M., Nuristani, N., & Hashmi, A. (2024). A hybrid machine learning model with self-improved optimization algorithm for trust and privacy preservation in cloud environment. *Journal of Cloud Computing, 13*(1), Article 157. https://doi.org/10.1186/s13677-024-00717-6

19. Sajadieh, S. M. M., & Noh, S. D. (2025). A review of digital twin integration in circular manufacturing for sustainable industry transition. *Sustainability, 17*(16), Article 7316. https://doi.org/10.3390/su17167316
20. Wu, Y., & Fu, X. (2026). Clean and smart energy technologies for agricultural energy internet systems: A comprehensive review and future perspectives. *Applied Sciences, 16*(10), Article 4859. https://doi.org/10.3390/app16104859
21. Zhang, S., Li, J., Shi, L., Ding, M., Nguyen, D. C., Chen, W., & Han, Z. (2025). Industrial metaverse: Enabling technologies, open problems, and future trends. *IEEE Communications Surveys & Tutorials*. Advance online publication. https://doi.org/10.1109/COMST.2025.3563919