International Journal of Scientific Research & Engineering Trends
Volume 11, Issue 2, Mar-Apr-2025, ISSN (Online): 2395-566X

An Adaptive Cloud–Edge Security Framework For Smart Manufacturing

Vanaja Kumari Degala
Academic Consultant, Dept of Computer Science (MCA),
SVU college of CM & CS, SV University, Tirupati -517501, AP, India.

Abstract- The rapid evolution of smart manufacturing systems has intensified the adoption of cloud–edge computing architectures to support real-time data processing, resource sharing, and intelligent decision-making. However, the convergence of heterogeneous devices, distributed services, and cross-domain interactions introduces complex security challenges that traditional perimeter-based protection models fail to address effectively. This paper presents an adaptive security framework for cloud edge enabled smart manufacturing environments based on zero-trust principles. The proposed framework integrates identity-centric access control, continuous trust evaluation, intelligent anomaly detection, and distributed data protection mechanisms to ensure secure interactions across cloud, edge, and terminal layers. Unlike static security architectures, the proposed approach dynamically adjusts access privileges and protection policies based on contextual risk assessment. The framework enhances system resilience against unauthorized access, data leakage, and lateral movement attacks while supporting scalability and cross-domain collaboration. Conceptual analysis demonstrates that the proposed framework provides proactive and fine-grained security protection suitable for next-generation manufacturing ecosystems.

Keywords – Smart manufacturing, cloud–edge computing, zero trust security, adaptive access control, industrial cybersecurity.

I. INTRODUCTION

Smart manufacturing systems increasingly rely on cloud–edge computing infrastructures to enable intelligent production, predictive maintenance, and real-time operational control. The integration of cloud platforms with edge processing units allows manufacturing enterprises to achieve low-latency responses while maintaining centralized resource management. At the same time, industrial environments now incorporate a large number of connected devices, sensors, control systems, and service platforms operating across organizational and network boundaries.

This architectural evolution significantly expands the system attack surface. Manufacturing systems are exposed to threats such as unauthorized device access, identity compromise, insecure application programming interfaces (APIs), data tampering, and supply-chain–based attacks. Conventional security models that depend on fixed network boundaries and static authorization rules are insufficient in such dynamic and distributed environments.

To address these challenges, this paper proposes an adaptive security framework for cloud edge enabled smart manufacturing systems grounded in the zero-trust security paradigm. The framework shifts security enforcement from network-centric protection to identity-driven and behaviour-aware control. By combining continuous trust assessment, intelligent monitoring, and distributed data protection, the proposed solution aims to provide active and scalable security for modern manufacturing ecosystems.

The main contributions of this work are:

1. The design of an adaptive zero-trust security framework tailored for cloud–edge smart manufacturing systems.
2. A dynamic access control mechanism based on continuous identity and behaviour evaluation.
3. An integrated approach to anomaly detection and secure data management across cloud, edge, and terminal layers.

II. RELATED WORKS

Existing research on industrial cybersecurity primarily focuses on perimeter defense, network isolation, and static access control mechanisms. Firewalls, intrusion detection systems, and role-based access control models have been widely adopted in traditional manufacturing networks. While these techniques provide baseline protection, they lack flexibility in environments characterized by frequent device mobility, service composition, and cross-domain interactions.

Recent studies have explored security architectures for cloud manufacturing and industrial Internet of Things (IIoT) systems. These works emphasize secure virtualization, trusted computing environments, and identity management solutions. Blockchain-based approaches have also been proposed to improve data integrity and traceability in distributed manufacturing systems. However, many existing solutions treat security as an add-on component rather than an integral and adaptive system capability.

Zero-trust security has emerged as a promising paradigm for addressing dynamic and distributed environments. By enforcing continuous verification and least-privilege access, zero-trust models reduce reliance on implicit trust derived from network location. Nevertheless, applying zero-trust concepts to cloud–edge smart manufacturing systems requires careful integration with industrial processes, real-time constraints, and heterogeneous devices. This paper addresses this gap by proposing a unified and adaptive security framework specifically designed for manufacturing scenarios.

III. SECURITY REQUIREMENTS OF CLOUD–EDGE SMART MANUFACTURING

Cloud–edge smart manufacturing systems consist of multiple interconnected layers, each with distinct security requirements:

Terminal and Device Layer: Manufacturing equipment, sensors, and controllers must be protected against unauthorized access, malware, and firmware manipulation. Secure identity binding and device integrity verification are essential.

Edge Processing Layer: Edge nodes perform real-time data processing and control functions. Security mechanisms must ensure isolation between services, protect computation environments, and detect abnormal behaviour.
Cloud Service Layer: Cloud platforms host manufacturing services, analytics engines, and data repositories. Access control, data confidentiality, and secure multi-tenancy are critical concerns.

Application and Service Layer: Manufacturing applications exchange sensitive operational data across domains. Secure APIs, service authentication, and auditability are required.
Data Lifecycle Management: Manufacturing data must be protected throughout acquisition, transmission, processing, storage, and sharing, with mechanisms for integrity verification and traceability.

These requirements highlight the need for a security architecture that is identity-centric, adaptive, and capable of unified enforcement across all layers.

IV. PROPOSED ADAPTIVE ZERO-TRUST SECURITY FRAMEWORK

The proposed system introduces an adaptive zero-trust–based security framework for cloud edge enabled smart manufacturing environments. Unlike traditional perimeter-based security models, the proposed approach assumes that no entity user, device, or service is inherently trusted. Every access request is continuously verified based on identity, device status, and behavioural context.

The framework integrates cloud services, edge computing nodes, and industrial devices under a unified security management layer. Security decisions are enforced dynamically using zero-trust policies, enabling secure data exchange and access control across heterogeneous manufacturing environments.

A. Framework Overview

The proposed framework adopts zero-trust principles to establish a unified security control plane spanning cloud, edge, and terminal components. Instead of relying on static trust assumptions, every access request is evaluated dynamically based on identity, device state, behaviour, and contextual risk.

The framework consists of:

- A unified identity and trust management module
- Continuous access evaluation and policy enforcement
- Intelligent monitoring and anomaly detection
- Distributed data protection mechanisms

B. SYSTEM ARCHITECTURE

The proposed system consists of four main components: the Device Layer, Edge Layer, Cloud Layer, and Security Management Module, as shown in Fig. 1.

1) DEVICE LAYER

The device layer includes industrial machines, sensors, controllers, and IoT devices deployed on the factory floor. Each device is assigned a unique identity and undergoes authentication before accessing system resources. Local processing is performed to support real-time operations while ensuring secure communication with edge nodes.

2) EDGE LAYER

The edge layer provides low-latency security enforcement close to data sources. It performs access control, data encryption, and anomaly detection to prevent unauthorized activities and reduce attack propagation.

3) CLOUD LAYER

The cloud layer manages centralized identity services, global policy enforcement, and secure data storage. It supports analytics-driven security updates and cross-domain coordination.

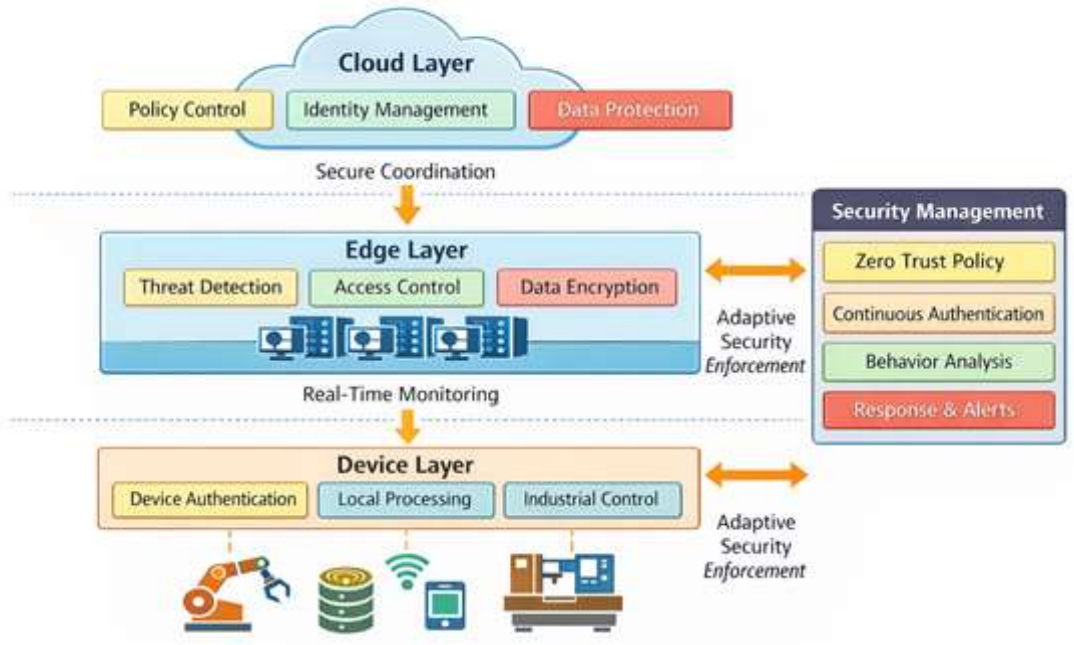

Fig. 1. Proposed adaptive cloud-edge security architecture for smart manufacturing systems.

4) SECURITY MANAGEMENT MODULE
This module enforces zero-trust policies through continuous authentication, trust evaluation, behaviour analysis, and incident response. Security decisions are dynamically updated based on real-time monitoring results.

C. DYNAMIC ACCESS CONTROL MECHANISM
Access decisions are made through continuous trust evaluation rather than one-time authentication. User and device identities are verified using multi-factor authentication, while behavioural attributes such as access patterns and system health are monitored in real time. Access privileges are adjusted dynamically to minimize risk exposure.

D. INTELLIGENT ANOMALY DETECTION
Machine-learning–based anomaly detection models are employed at the edge and cloud layers to identify abnormal sensor readings, network traffic patterns, and user behaviors. By correlating multi-source security data, the framework enables early detection of potential attacks and operational faults.

E. SECURE DATA MANAGEMENT
To enhance data integrity and traceability, the framework incorporates distributed ledger techniques for critical manufacturing data. Cryptographic protection and classification-based policies ensure that sensitive information is accessed and shared only by authorized entities.

V. DISCUSSION AND ANALYSIS

The proposed framework improves security posture by eliminating implicit trust and enabling fine-grained control over system interactions. Adaptive access policies reduce the impact of compromised identities, while intelligent monitoring enhances situational awareness. Compared with traditional static security architectures, the framework provides improved resilience against lateral movement attacks and cross-domain threats.

Furthermore, the modular design allows the framework to scale with system growth and integrate with existing industrial platforms. While implementation complexity and computational overhead must be considered, the benefits in terms of security robustness and flexibility outweigh these challenges.

A. Disadvantages of Existing Systems
Existing perimeter-based and static security models suffer from several limitations:

- Implicit trust based on network location
- Inability to adapt to dynamic industrial environments
- Limited visibility across cloud–edge layers

- Vulnerability to lateral movement and insider attacks

B. Advantages of the Proposed System

The proposed framework offers:

- Continuous verification and fine-grained access control
- Adaptive security policies based on contextual risk
- Improved detection of advanced and insider threats
- Scalability and compatibility with existing industrial platforms

VI. CONCLUSION

This paper presented an adaptive zero-trust–driven security framework for cloud–edge–enabled smart manufacturing systems. By integrating continuous trust evaluation, intelligent anomaly detection, and secure data management, the framework addresses the limitations of traditional perimeter-based security models. The proposed approach supports dynamic, scalable, and proactive protection suitable for next-generation manufacturing environments. Future work will focus on prototype implementation and performance evaluation in real industrial scenarios.

Future work will focus on implementing a real-world prototype of the proposed framework and evaluating its performance using industrial datasets. Further research will explore lightweight security mechanisms for resource-constrained devices and the integration of advanced artificial intelligence techniques for enhanced threat prediction and response.

REFERENCES

1. M. Rusdan and I. Ramlan, “Approach of Zero Trust Security to Improve Internet of Things Infrastructure Security,” *LogicLink*, vol. 2, no. 2, pp. 1–10, 2025.
2. M. A. Rahman, M. A. Hossain, and E. Hossain, “ZERO-TRUST Access Control Architecture for Privacy-Preserving Machine Learning in Smart Edge Networks,” *Int. J. Eng. Res. Sci. Tech.*, vol. 15, no. 4, pp. 114–122, 2025.
3. J. Deng, X. Li, and Y. Zhang, “Toward Zero Trust in 5G Industrial Internet Collaboration Systems,” *Digital Commun. Netw.*, vol. 11, no. 2, pp. 158–169, May 2025.
4. S. Yi, C. Li, and Q. Li, “A Survey of Security Architectures for Edge Computing-Based IoT,” *Internet of Things*, vol. 3, no. 3, pp. 19–43, 2022.
5. T. Nguyen, L. Luo, and B. L. Mark, “A Zero-Trust Architecture for Remote Access in Industrial IoT Infrastructures,” *Electronics*, vol. 12, no. 3, Art. no. 566, Mar. 2025.
6. F. Zhang, K. Lin, and P. Wang, “Future Industry Internet of Things with Zero-Trust Security,” *Inf. Syst. Front.*, vol. 24, pp. 101–120, Jan. 2024.
7. J. Sengupta, S. Ruj, and S. D. Bit, “A Secure Fog Based Architecture for Industrial Internet of Things and Industry 4.0,” *arXiv preprint arXiv:2005.07147*, May 2020.
8. S. Ma, P. Wang, and F. Gao, “Privacy-Preserving Anomaly Detection in Cloud Manufacturing via Federated Transformer,” *arXiv preprint arXiv:2204.00843*, Apr. 2022.