

GENERATIVE AI-POWERED AUTONOMOUS CYBERSECURITY FRAMEWORKS FOR INDUSTRIAL IOT ENVIRONMENTS: ENHANCING THREAT INTELLIGENCE, SECURE COMMUNICATION, AND ADAPTIVE DEFENSE MECHANISMS

Ari Pratama Santoso¹ & Budi Hartono²

¹Department of Computer Science and Engineering, Indian Institute of Technology Delhi (IIT Delhi), New Delhi 110016, Delhi, India

²Department of Computer Science and Engineering, Indian Institute of Technology Madras (IIT Madras), Chennai 600036, Tamil Nadu, India

ABSTRACT

The rapid adoption of the Industrial Internet of Things (IIoT) has improved industrial automation, operational efficiency, and real-time decision-making, but it has also increased exposure to sophisticated cyber threats targeting interconnected devices and critical infrastructure. Traditional cybersecurity mechanisms often struggle to detect and respond to evolving attacks in dynamic IIoT environments, creating a need for intelligent and adaptive security solutions. This study proposes a Generative AI-powered autonomous cybersecurity framework that integrates intelligent threat intelligence, secure communication, and adaptive defense mechanisms to enhance the resilience of IIoT networks. The research employs a comprehensive literature-based analytical methodology to examine existing AI-driven cybersecurity approaches, identify current limitations, and develop a unified conceptual framework for proactive cyber defense. The proposed framework combines generative AI with continuous threat monitoring, cryptographic protection, autonomous decision-making, and adaptive response capabilities to improve threat detection, reduce response latency, and strengthen secure data transmission. The findings indicate that integrating generative AI into autonomous cybersecurity architectures significantly enhances threat prediction, intelligent anomaly detection, and overall network resilience compared with conventional security approaches. This research contributes a scalable and intelligent security framework that provides practical guidance for strengthening cybersecurity in next-generation Industrial IoT environments.

KEYWORDS: Generative AI, Industrial Internet of Things (IIoT), Autonomous Cybersecurity, Threat Intelligence, Secure Communication, Adaptive Defense, Large Language Models (LLMs), Industrial Control Systems.

Article History

Received: 08 Mar 2026 | Revised: 10 Mar 2026 | Accepted: 14 Mar 2026
