Chapter 12
AI and Blockchain Synergy: Enhancing Security in Industrial Automation

Himanshu Tyagi
https://orcid.org/0009-0001-8435-9832
Quantum University, India

Pawan Kumar Goel
https://orcid.org/0000-0003-3601-102X
Raj Kumar Goel Institute of Technology, Ghaziabad, India

Akansha Gautam
https://orcid.org/0000-0003-4017-872X
Tula's Institute, India

Abhishek Agarwal
Quantum University, India

Sandhya Samant
https://orcid.org/0000-0002-9538-5964
COER University, India

ABSTRACT

This chapter explores the convergence of AI and blockchain in industrial automation, highlighting advancements in security, efficiency, and transparency. It outlines AI's role in predictive maintenance, anomaly detection, and intelligent decision-making, alongside blockchain's strengths in data integrity, tamper-proof records, and automated compliance. A multi-layered architecture is proposed for seamless integration, addressing scalability, complexity, and legal hurdles. Real-world use cases include secure predictive maintenance, fraud detection, decentralized identity, and supply chain automation. Emerging trends such as federated learning, AI-powered smart contracts, and zero-trust architectures are also discussed, showcasing the transformative potential of combining AI and blockchain.

DOI: 10.4018/979-8-3373-3241-3.ch012

1. INTRODUCTION

Industrial automation has revolutionized the manufacturing and production sectors by replacing manual operations with intelligent machines, sophisticated control systems, and data-driven processes. This transformation enhances efficiency, precision, and consistency in operations while simultaneously reducing human errors and operational costs. However, as industrial systems become increasingly interconnected through IoT devices, cloud platforms, and smart sensors, the potential for cyber threats has expanded significantly (Bagheri & Jin, 2020).

The confluence of operational technology (OT) and information technology (IT) presents both remarkable opportunities and serious cybersecurity challenges. Traditional security measures often fall short when it comes to addressing advanced persistent threats (APTs), insider attacks, data tampering, and unauthorized access within complex automated environments (Anderson & Sharifi, 2021).

To tackle these vulnerabilities, a new wave of emerging technologies—most notably Artificial Intelligence (AI) and Blockchain—has begun to reshape the landscape of industrial cybersecurity. This chapter delves into how the synergy of AI and Blockchain can create a comprehensive, rugged, and intelligent security skeleton for industrial automation.

1.1. Overview of Industrial Automation

This involves the integration of control systems, such as computers, robots, and information technologies, to manage handle processes and machinery across industries. It plays a key important role in:

a) Boosting productivity and operational effectiveness
b) Reducing human intervention and labor costs
c) Improving quality control and precision
d) Streamlining complex workflows through intelligent decision-making

Modern industrial automation spans a variety of sectors, including manufacturing, oil and gas, logistics, energy, and pharmaceuticals. With the emergence of Industry 4.0, these systems are increasingly reliant on data, sensors, and connectivity, making cybersecurity a paramount concern (Balducci & Mancuso, 2020).

1.2. Current Security Challenges in Industrial Systems

Despite the numerous benefits, industrial automation systems are confronted with an escalating array of cyber threats due to:

a) Increased connectivity: OT networks are becoming more interconnected with IT systems and the internet, exposing them to external attacks.
b) Legacy systems: Many industrial systems still operate on outdated software or hardware that lacks modern security features.
c) Insufficient authentication and access controls: Weak or default credentials often remain unchanged, creating vulnerabilities.