Chapter 21
Security Fortifying Critical Infrastructure:
AI-Based Identity and Access Management (IAM) for Industrial Automation

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

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

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

Aafia Hussain
https://orcid.org/0009-0004-2975-4938
College of Engineering, Roorkee, India

ABSTRACT

Industrial automation has created a new era of connected systems, making strong security essential. Traditional Identity and Access Management (IAM) systems, though once effective, now struggle with the evolving demands of complex industrial environments. Static IAM approaches fall short as networks expand, highlighting the need for intelligent, adaptive solutions. AI introduces dynamic, context-aware security through technologies like machine learning, deep learning, behavioral biometrics, and anomaly detection. These enable continuous authentication, real-time access control, and improved identity verification. This work explores AI-driven IAM in sectors such as manufacturing and energy, outlining benefits like enhanced threat detection, compliance, operational resilience, and faster response. Challenges include data protection, legacy system integration, and scalability. Future directions include blockchain-based identity, Federated Learning, Explainable AI, and insider threat detection—ensuring AI-powered IAM evolves to meet the future of industrial cybersecurity.

DOI: 10.4018/979-8-3373-3241-3.ch021

1. INTRODUCTION

1.1. Overview of Industrial Automation

Industrial automation is the process of managing and running industrial processes with little to no human involvement by using control systems like computers, robotics, and information technology. It includes a number of industries, such as essential infrastructure, manufacturing, energy, and oil & gas. Industrial processes are supported by essential components such as Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs), and Supervisory Control and Data Acquisition (SCADA) systems.

Industries can achieve more efficiency, lower prices, better quality, and increased safety by automating complicated processes and repetitive jobs. Strong security measures are necessary since these systems are more susceptible to cyberattacks as a result of their increased interconnection via cloud and Industrial Internet of Things (IIoT) technologies (Deepak, Gulia, Gill, & Yahya, 2024).

1.2. Importance of Identity and Access Management (IAM)

Identity and Access Management (IAM) is a foundational element of cybersecurity (Fernandes et al., 2014) that controls who can access specific resources and under what conditions.

a) In industrial automation, IAM ensures that only authorized personnel and devices can interact with critical systems and sensitive data.
b) Effective IAM safeguards against insider threats, unauthorized access, and external cyberattacks, thereby protecting operational continuity and overall safety.
c) IAM helps organizations comply with important regulatory standards such as IEC 62443, NIST cybersecurity guidelines, and GDPR (Stouffer et al., 2011).
d) In complex and high-stakes industrial settings, where security breaches could cause catastrophic consequences, robust IAM systems are essential to maintain trust, security, and operational resilience.

1.3. Role of Artificial Intelligence (AI) in Modern IAM

The majority of traditional IAM systems are static and rule-based (Abomhara & Køien, 2015). They find it difficult to stay on top of the constantly changing and dynamic world of cybersecurity threats. Static access policies and manual rule construction are unable to react swiftly to complex attacks.

a) AI gives IAM systems flexibility, intelligence, and automation. It makes it possible for IAM platforms to constantly adapt to new threats and learn from trends.
b) AI has real-time access to data and is capable of processing and analyzing enormous amounts of identity. It assists in identifying irregularities in user behavior that can point to insider threats or compromised accounts.
c) Using threat intelligence, past access data, and behavioral patterns, AI models are able to forecast possible security breaches. Rather than depending only on reactive tactics, predictive analytics improves proactive defense options.