Chapter 17
AI Based IAM For Industrial Automation:
Securing IIoT, ICS, and OT Systems

Vatsal Gupta
https://orcid.org/0009-0007-0732-9895
Apple, USA

ABSTRACT

This chapter explores the transformative role of Artificial Intelligence (AI) in strengthening Identity and Access Management (IAM) for industrial automation, aligned with the evolving security demands of Industry 4.0. It details how AI technologies—such as Machine Learning, Deep Learning, and Behavioral Analytics—enhance identity verification, access control, and threat detection across IIoT, ICS, and OT systems. Case studies from Siemens, Equinor, and Tesla showcase real-world applications, highlighting improved security and operational efficiency. The chapter also addresses challenges like adversarial AI, data privacy, and legacy integration, offering solutions including federated learning and blockchain. It concludes with insights into emerging trends like quantum computing, providing cybersecurity professionals and policymakers a forward-looking perspective on AI-driven IAM in industrial environments.

INTRODUCTION

Identity and Access Management (IAM) serves a critical function in cybersecurity by managing who or what should have access to essential systems, data, and organizational resources. In today's industrial landscape, the role of IAM is more critical than ever due to the interconnected nature of physical processes, operational technologies and digital networks. Industrial Internet of Things (IIoT) and Industrial Control Systems (ICS) technologies together with Operational Technology (OT) environments within the Industry 4.0 framework require continuous connectivity and real-time data exchange. Such interdependence increases the risk surface which makes it essential to establish an effective IAM program to guard sensitive assets from unauthorized access, advanced cyberattacks and insider threats.

Traditionally, IAM in industrial settings involved usage of more static methods like roles, passwords and access privileges that remain fixed until manually updated. While this has been effective in less dynamic environments, the modern industrial environments require something more dynamic. For in-

DOI: 10.4018/979-8-3373-3241-3.ch017

stance, there can be thousands of IIoT devices in these environments in the form of sensors, actuators and Programmable Logic Controllers (PLCs), each requiring unique access control. Similarly, ICS and OT which often control critical infrastructure like power grids, water treatment plants, and manufacturing lines, can be exposed to various types of threats and therefore, have very little margin of error. The limitations of traditional IAM are becoming more evident as industrial systems are experiencing evolving threats like ransomwares targeting OP networks, supply chain attacks due to weak authentication and misuse of excessive privileges by an insider.

The advent of Artificial Intelligence (AI) marks a paradigm shift in IAM, offering intelligent, adaptive, and proactive solutions to tackle the threats relevant to modern industrial environments. AI functions as a bridge that can be leveraged by modern IAM professionals to close the gap between traditional IAM solutions and the needs of today's interconnected and security-challenged environments. AI powered IAM can leverage Machine Learning (ML), Deep Learning (DL), and behavioral analytics to dynamically assess identities, monitor access patterns, and respond to anomalies in real time. AI also delivers advanced identity verification capabilities along with adaptive access management and self-learning identity governance to ensure secure and resilient operations. By integrating AI, IAM evolves from a static gatekeeper into a predictive and resilient framework capable of anticipating threats before they materialize.

The importance of AI-based IAM in industrial automation cannot be overstated. Imagine someone gaining unauthorized access to a PLC or compromising SCADA (Supervisory Control and Data Acquisition) system - one can halt production in any company while the other scenario puts public safety in danger. One of the examples of vulnerable OT systems is the 2021 Colonial Pipeline ransomware attack, where credential-based exploits led to disruption of the fuel supply across the U.S. East Coast (CISA, 2021). AI-driven IAM capabilities like continuous authentication, context-aware access control, and automated threat mitigation can alleviate some of the concerns. For example, an AI system might detect an employee attempting to access a restricted OT network from an unusual location or device, flagging it as a potential insider threat and revoking access instantaneously.

Similarly, let's go back to the IIoT ecosystem as an example. A typical smart factory might deploy thousands of interconnected devices where each device communicates with central systems and external networks. Traditional IAM struggles to manage this complexity, often requiring manual configuration for each device - a process prone to human error and scalability issues. AI-based IAM, by contrast, can automatically profile devices, assign access privileges based on their roles, and monitor their interactions for signs of compromise. If a sensor begins transmitting data outside its normal parameters, AI can isolate it from the network, preventing potential exploitation. This level of granularity and responsiveness is critical in industrial automation, where even minor disruptions can lead to significant financial or operational losses.

Moreover, the stakes in ICS and OT environments extend beyond financial considerations to include safety and regulatory compliance. A breach in a chemical plant's control system, for instance, could trigger hazardous material releases, endangering workers and communities. Regulatory frameworks like NIST 800-82 (Guide to Industrial Control Systems Security) and IEC 62443 (guidelines for securing industrial automation and control systems (IACS) and OT networks) emphasize the need for robust access controls, yet traditional IAM often falls short in meeting these standards dynamically. AI enhances compliance by providing auditable logs of access events, real-time risk assessments, and automated policy enforcement - features that align with both security and legal requirements.