Chapter 13
Real-Time AI-Based Security Monitoring for Industrial Control Systems

Saurabh Singhal
Engineering Institute, Greater Noida Institute of Technology, India

Sandeep Singh Sikarwar
Maldives Business School, Malé, Maldives

Ajeet Kumar Sharma
Sharda School of Computing Sciences and Engineering, Sharda University, Greater Noida, India

Aman Kumar Kumar
Sharda School of Computing Sciences and Engineering, Sharda University, Greater Noida, India

Avinash Kumar Kumar Sharma
https://orcid.org/0000-0001-6762-6778
Sharda School of Computing Sciences and Engineering, Sharda University, Greater Noida, India

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

ABSTRACT

Industry systems controlling power generation operations together with water distribution and manufacturing facilities form a connected network similar to a massive web infrastructure. The Industrial Control Systems referred to as ICS serve vital functions although they remain at constant risk of stealthy cyberattacks. Hacker strikes result in more than financial loss and temporary shutdowns since they endanger human lives. Modern defenses based on firewalls or intrusion detection systems have become insufficient to protect industrial systems. Real-Time AI-Based Security Monitoring emerges to rescue operations through its rescue mission. A super-smart guard dog equipped with machine learning and deep learning analyses suspicious activity by detecting abnormal user behavior to arrest offenders while performing automatically in real-time operations. Unlike ordinary systems that depend on set rules this AI system acquires information directly from its past activities while shifting its detection methods to face new hacker strategies.

DOI: 10.4018/979-8-3373-3241-3.ch013

1. INTRODUCTION

The fundamental core of critical infrastructure sectors depends on Industrial Control Systems (ICS) to control operations in power systems and manufacturing and water treatment facilities and others. The rising digital development and extensive network connections make ICS systems more vulnerable to cybersecurity threats that disrupt critical operational services. Yearly security controls prove inadequate to stop advanced security threats thus making real-time artificial intelligence-based security monitoring an absolute necessity. Organizations benefit from artificial intelligence because it lets them spot irregularities as well as predict hacking threats while enabling automatic incident response functions. Power generation along with manufacturing production facilities and oil and gas facilities and water treatment plants and transportation systems depend on Industrial Control Systems (ICS) as their critical foundation (Bhamare, Deval, et al, 2020). These systems execute automated monitoring along with process control to deliver capabilities related to safety and efficiency and reliability. The three main components of ICS include SCADA systems together with Distributed Control Systems (DCS) and Programmable Logic Controllers (PLC) (Gaiceanu, Marian, et al.,2020). Industrial Control Systems maintained isolation from outside networks until technology advances from digitalization and Industrial Internet of Things and remote connections brought ICS controllers into contact with enterprise IT infrastructure and cloud computing platforms. A combination of operational benefits from integration such as predictive maintenance and real-time monitoring creates security vulnerabilities which cyber attackers can abuse. Modern-day reality shows ICS cyberattacks leading to serious operational damages.

Vulnerabilities in the system enable these attacks through methods including ransomware breaches and data breaches alongside disruptive Denial-of-Service incidents. Special operational constraints characterize ICS frameworks because they must handle legacy equipment while running continuously and as they combine IT systems with Operational Technology (OT) (Makadia et al.,2022). Modern industrial control systems face many cyber threats while maintaining them becomes complicated because of system interruptions. The connection between IT and OT is expanding which creates larger threats areas allowing cyber dangers to move from business systems all through ICS infrastructure. Most ICS operators along with engineer's value operational efficiency over cybersecurity so gaps in security preparedness develop as a result. The crucial nature of ICS security demands improvement after notorious incidents like Stuxnet Triton and Colonial Pipeline which led organizations to adopt Artificial Intelligence (AI) as their real-time protection system. (Kumar, Sumit et al.,2025).

The detection of security threats is being revolutionized through Artificial Intelligence because it provides automatic systems which utilize intelligence and proactively find threats. Security monitoring systems operated by Artificial Intelligence base their threat detection on machine learning together with deep learning and behavioural analytics to automatically identify irregularities while spotting suspicious activities in real-time. The primary advantages include anomaly finding and predictive threat evaluation and automatic incident response and adaptive learning technologies. AI systems acquire normal operational patterns from data which enables them to detect irregularities while also predicting forthcoming risks through forecasting so they can automatically handle incidents and stop newly developed attack techniques. Companies gain the ability to transition their cybersecurity approach from reactive to proactive through the combination of ICS security with AI implementation.

ICCS infrastructure requires real-time security monitoring as a fundamental measure to handle threats that protect system operational functions from disruption. IDS and SIEM systems lack the capability to handle dynamic cyberattacks because of their inability to confront such characteristics. Time-sensitive