Chapter 22
AI-Powered Digital Forensics for Industrial Cyber Incidents

P. Selvakumar
https://orcid.org/0000-0002-3650-4548
Department of Science and Humanities, Nehru Institute of Technology, Coimbatore, India

K. Gandhimathi
PSGR Krishnammal College for Women, India

Anjali
https://orcid.org/0009-0000-3456-9893
United College of Engineering and Research, Prayagraj, India

P. Sudheer
https://orcid.org/0009-0005-1912-6636
CVR College of Engineering, India

Nilesh Anute
https://orcid.org/0000-0001-6599-813X
Sri Balaji University, India

T. C. Manjunath
https://orcid.org/0000-0003-2545-9160
Rajarajeswari College of Engineering, India

ABSTRACT

The increasing digitization of industrial control systems (ICS) and critical infrastructure has made these environments prime targets for cyber threats. Traditional digital forensic methodologies (AI) and machine learning (ML) to automate data analysis, accelerate threat detection, and enhance forensic accuracy. and mitigating cyber incidents across industrial sectors, including energy, manufacturing, utilities, and transportation AI-powered digital forensics enhances industrial cybersecurity by automating threat detection, identifying anomalous behavior in ICS networks, and uncovering, and operational technology (OT) environments to identify malicious and real-time incident response to prevent operational downtime. Additionally, AI-powered behavioral analytics help detect insider threats by correlating multi-source industrial data to identify suspicious user activity, unauthorized command execution, and compromised credentials

DOI: 10.4018/979-8-3373-3241-3.ch022

INTRODUCTION TO INDUSTRIAL CYBER INCIDENTS: THE GROWING THREAT LANDSCAPE

In today's digital era, industrial cyber incidents have emerged as a pressing concern for organizations worldwide, particularly those operating in critical interconnected landscape where cyber threats can have far-reaching consequences beyond traditional data breaches. Unlike conventional cyberattacks that primarily target data integrity and confidentiality, industrial cyber incidents pose a direct threat to physical processes, (Battiato et al., 2012) safety, and national security. The increasing sophistication of threat actors, ranging from state-sponsored groups to cybercriminals and hacktivists, has further exacerbated the risk, necessitating a paradigm shift in cybersecurity strategies to protect industrial systems from potentially catastrophic disruptions. Over the past decade, industrial environments have undergone rapid digital transformation, embracing automation, IT environments. Unfortunately, many legacy industrial systems were not designed with cybersecurity in mind, making them highly vulnerable to modern cyber threats. Attackers are exploiting these weaknesses to disrupt industrial operations, cause physical damage, and, in some cases, hold critical infrastructure hostage through ransomware attacks. One of the most alarming aspects of industrial cyber incidents is the growing number of state-sponsored attacks targeting critical infrastructure. Nation-state actors are leveraging cyber capabilities to conduct espionage, sabotage, and even cyber warfare against geopolitical adversaries.(Butterfield et al., 2018) These incidents underscore the urgent need for industrial organizations to adopt robust cybersecurity frameworks, implement proactive threat detection mechanisms, and enhance collaboration between the public and private sectors to mitigate risks and industrial networks. The infamous SolarWinds attack demonstrated how a compromised software update could lead to widespread infiltration of critical systems. Similarly, the increasing use of artificial intelligence and machine learning in cyberattacks enables threat actors to automate reconnaissance, exploit vulnerabilities at scale, and evade traditional security defenses. This rapidly evolving threat landscape requires organizations to rethink their cybersecurity approaches, integrating advanced technologies such as behavioral analytics, threat intelligence, and machine learning-based anomaly detection and securing industrial environments. Compliance with these frameworks is no longer optional; it is a necessity for organizations seeking to protect their operations, comply with regulatory requirements, and maintain stakeholder trust. Additionally, cybersecurity insurance has gained traction as a risk management tool, helping organizations mitigate financial losses resulting from cyber incidents. Despite these efforts, the fostering a security-conscious culture where personnel are vigilant against potential threats. Furthermore, collaboration between IT and OT teams is crucial to bridging the gap between traditional cybersecurity practices and industrial security requirements. Historically, IT and OT have operated in silos, leading to misaligned security priorities. A unified approach that integrates IT security best practices with OT-specific risk management strategies is essential for defending against modern industrial cyber threats. Looking ahead, the future of industrial cybersecurity will be shaped by emerging trends such as technology offers promising applications in securing industrial supply chains, ensuring data integrity, and preventing unauthorized modifications to critical system configurations. Autonomous cyber defense systems, powered by artificial intelligence, will play a crucial role in automating threat detection, incident response, and remediation, reducing the reliance on human intervention. In conclusion, the growing threat landscape of industrial cyber incidents demands a proactive, multi-layered approach to cybersecurity. As industrial environments continue to evolve,, ensuring the protection of critical infrastructure against the ever-increasing cyber threats of