Chapter 6
Deep Learning for Anomaly Detection in Industrial Networks

Ayush Tripathi
https://orcid.org/0009-0007-6869-0588
Sharda University, India

Prashant Upadhyay
https://orcid.org/0000-0002-9257-9181
Sharda University, India

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

ABSTRACT

As industrial networks have become increasingly complex, they have become the target of choice for cyber attacks, and thus there is a need for sophisticated anomaly detection mechanisms. This chapter delves into deep learning-based solutions to detect and mitigate cyber attacks in Industrial IoT (IIoT) and Industrial Control Systems (ICS). Utilizing methods such as autoencoders, recurrent neural networks (RNNs), and convolutional neural networks (CNNs), deep learning systems are able to identify anomalies from normal network operations in real time. The chapter covers supervised and unsupervised learning methods, feature engineering's role, the challenges posed by dataset availability, adversarial attacks, and explainability in industrial anomaly detection. Industrial applications and case studies illustrate how deep learning improves industrial cybersecurity through adaptive, scalable, and smart threat detection

INTRODUCTION

Industrial networks have been revolutionized in the last few years with fast-paced developments in automation, connectivity, and artificial intelligence. These networks, including Industrial Control Systems (ICS) and the Industrial Internet of Things (IIoT), are the backbone of contemporary industries like manufacturing, energy generation, healthcare, and transportation. In contrast to conventional IT networks, which are mainly concerned with data storage and processing, industrial networks are tasked with the

DOI: 10.4018/979-8-3373-3241-3.ch006

direct control and operation of physical processes. They enable real-time communication among sensors, actuators, programmable logic controllers (PLCs), distributed control systems (DCS), and human-machine interfaces (HMIs). This smooth interaction between hardware and software has allowed industries to maximize production efficiency, minimize operational expenses, and adopt predictive maintenance practices. Yet, as industrial networks become more networked and dependent on digital technologies, they have also become more exposed to cyber threats. Nation-state attackers and cybercrime groups, among other malicious actors, have identified the strategic interest of attacking industrial infrastructure, since successful intrusions can have devastating consequences, including widespread production breakdowns, environmental risks, and loss of human life. Recent research highlights the growing sophistication of cyberattacks targeting industrial networks, emphasizing the need for advanced security frameworks to mitigate these risks (Asghar et al. 2019). The increasing sophistication of industrial systems, coupled with their importance in national security and economic stability, has placed industrial stakeholders at the forefront of cybersecurity concerns.

Cyber attacks on industrial networks have developed markedly over the last decade, presenting unprecedented challenges to conventional security measures. Industrial networks were first designed as stand-alone systems, quite frequently on proprietary protocols with little exposure to the outside world. But the use of cloud computing, edge computing, and remote access solutions has obscured the distinction between operational technology (OT) and information technology (IT) environments. This intersection has widened the attack surface, exposing industrial systems to cyber incursions. As opposed to traditional IT networks, where security compromise can lead to data loss or monetary losses, cyberattacks on industrial networks have serious real-world implications. For example, a cyber attack on a power grid can stop electricity supply to millions of homes, whereas an attack on a chemical plant can result in leakage of dangerous material and ecological catastrophe. A study on the evolution of industrial cyber threats underscores the inadequacy of legacy security tools in addressing modern attack vectors, such as zero-day exploits and polymorphic malware (Tsiknas et al. 2021). Some of the latest cases, like the Stuxnet worm, Triton malware infection of safety instrumented systems, and ransomware attacks on factories, illustrate how sophisticated industrial cyber threats have become. Legacy cybersecurity tools, like rule-based intrusion detection systems (IDS) and signature-based antivirus software, are no longer adequate to safeguard industrial networks against these ever-changing threats. Legacy solutions depend on preknown attack signatures and heuristics and are, therefore, useless against zero-day exploits, polymorphic malware, and adversarial attacks. In addition to this, industrial settings suffer from strong real-time requirements, where any lag in detecting anomalies can have disastrous implications. In light of these challenges, a demand for smart, adaptive, and autonomous security solutions that can automatically detect and respond to cyber threats in real-time is increasingly being felt.

Deep learning has become the revolutionary technology within the industrial cybersec space to provide unparalleled capacity for anomaly detection, predictive insights, and threat blocking in real time. Compared to conventional machine learning models that heavily depend on feature engineering performed manually and on domain knowledge, deep learning models can learn directly from high-dimensional data to find significant patterns on their own. This capability particularly suits industrial cybersecurity, where traffic on the network, sensor output, and logs from control systems produce enormous amounts of unstructured data. Recent advancements in deep learning for industrial cybersecurity demonstrate the effectiveness of autoencoders and RNNs in detecting anomalies in real-time (Kabore et al. 2021). Autoencoders, recurrent neural networks (RNNs), and convolutional neural networks (CNNs) have proven to be highly effective for detecting cyber abnormalities as shown in Figure 1. by learning about the typical