RADemics

AI Based Security Solutions for Industrial Control Systems and SCADA Networks

R. Thiyagarajan, M. Arivamudhan, P. Shanmugaraja
Government College of Engineering, Annamalai University

AI Based Security Solutions for Industrial Control Systems and SCADA Networks

[1]R. Thiyagarajan, Associate Professor, Electronics and Communication Engineering, Government College of Engineering, Dharmapuri-636704. rajan.as.ece@gmail.com

[2]M. Arivamudhan, Professor, Electronics and Communication Engineering, Government College of Engineering, Dharmapuri-636704. aridhan.dh@gmail.com

[3]P. Shanmugaraja, Professor & Head, Electronics and Communication Engineering, Annamalai University, Chidambaram. shanmugaraja@gmail.com

Abstract

The rapid evolution of Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) networks has significantly increased the exposure of critical infrastructure to sophisticated cyber threats. Traditional cybersecurity measures often struggle to address the unique challenges posed by these systems, such as data privacy, scalability, and real-time threat detection. Federated learning, a decentralized machine learning paradigm, has emerged as a promising solution to enhance security in ICS/SCADA environments. By enabling local model training on distributed devices while maintaining data privacy, federated learning offers a secure, scalable, and efficient framework for real-time anomaly detection and collaborative threat mitigation. This chapter explores the integration of federated learning with edge computing to address the computational and resource constraints of Industrial Internet of Things (IIoT) devices, ensuring low-latency responses to emerging threats. The chapter further discusses the advantages of federated learning in enabling secure data sharing, improving system resilience, and complying with stringent data privacy regulations. With applications spanning predictive maintenance, intrusion detection, and threat intelligence, federated learning represents a pivotal advancement in securing ICS/SCADA networks. This chapter provides a comprehensive analysis of the role of federated learning in modern industrial cybersecurity, highlighting its potential to transform the landscape of threat detection and response in critical infrastructure systems.

Keywords: Federated Learning, ICS/SCADA Security, Industrial Internet of Things (IIoT), Anomaly Detection, Data Privacy, Edge Computing

Introduction

Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) networks are the backbone of critical infrastructure across various industries, including energy, manufacturing, transportation, and water management [1]. These systems facilitate the real-time monitoring and control of industrial processes, making them essential for ensuring operational efficiency, safety, and reliability [2]. However, as ICS/SCADA networks become more interconnected and reliant on digital technologies, their exposure to cybersecurity threats has significantly increased [3]. Cyberattacks targeting these systems can have devastating consequences, ranging from operational disruptions and financial losses to risks to public safety

and national security. Consequently, securing these systems against increasingly sophisticated cyber threats is an urgent priority for industries worldwide [4]. Traditional cybersecurity methods, including firewalls, intrusion detection systems, and centralized data analysis, often fail to effectively address the dynamic and distributed nature of ICS/SCADA networks, necessitating innovative solutions that can keep pace with evolving threats [5].

The rise of Industrial Internet of Things (IIoT) devices within ICS/SCADA environments further exacerbates the challenge of securing these systems [6]. IIoT devices generate vast amounts of data and are often deployed across geographically dispersed locations, making them difficult to monitor and protect using conventional security measures [7]. These devices are typically resource-constrained, with limited computational power, memory, and network bandwidth, which poses significant challenges for traditional data analysis techniques [8]. Moreover, the sheer volume of data generated by IIoT devices often overwhelms centralized systems, leading to delays in threat detection and response [9]. As a result, there is an increasing need for distributed, scalable, and privacy-preserving solutions that can efficiently process large datasets in real-time without compromising system performance or security [10].

Federated learning, a decentralized approach to machine learning, offers a promising solution to the cybersecurity challenges faced by ICS/SCADA networks [11]. Unlike traditional machine learning models, which rely on centralized data aggregation for training, federated learning allows models to be trained locally on devices or edge nodes [12]. Only model updates, rather than raw data, are shared with a central server, ensuring that sensitive operational data remains private and secure [13]. This privacy-preserving feature is particularly important in ICS/SCADA systems, where data privacy is critical due to regulatory requirements and the sensitivity of operational information [14]. Federated learning not only addresses privacy concerns but also enables continuous learning and adaptation across a distributed network, making it an ideal solution for enhancing security in dynamic industrial environments [15].