RADemics

Federated and Transfer Learning for Distributed Anomaly Detection in IoT-Enabled Power Electronics for Industrial Automation

S. Kanimozhi, R. Deebika, Ram N Hajare
PSG COLLEGE OF ARTS AND SCIENCE, K S R COLLEGE OF ENGINEERING, SANJIVANI COLLEGE OF ENGINEERING

6. Federated and Transfer Learning for Distributed Anomaly Detection in IoT-Enabled Power Electronics for Industrial Automation

[1]S. Kanimozhi, Assistant professor, Department of Electronics, PSG College of arts and science, Coimbatore, Tamilnadu, India. psgkanimozhi2019@gmail.com

[2]R. Deebika, Assistant Professor, Department of Computer Science and Engineering, K S R College of Engineering, Tiruchengode, Tamil Nadu, India, rdeebikame@gmail.com

[3]Ram N Hajare, Asstt. Prof. Electrical Engg dept, Sanjivani College of Engineering Kopargaon, ramnhajare@gmail.com

Abstract

The rapid integration of IIoT in power electronics has transformed industrial automation, enabling real-time monitoring, predictive maintenance, and intelligent decision-making. The distributed nature of IIoT-enabled power electronics introduces significant challenges in anomaly detection, including data heterogeneity, privacy concerns, and computational limitations of edge devices. Traditional centralized learning approaches are inefficient in handling these constraints, necessitating the adoption of decentralized learning paradigms. Federated Learning (FL) has emerged as a transformative approach, enabling collaborative model training across edge devices while preserving data privacy. FL faces challenges such as communication overhead, resource constraints, and performance degradation due to non-independent and identically distributed (non-IID) data. To address these limitations, Transfer Learning (TL) was integrated with FL to enhance model adaptability, enabling efficient knowledge transfer across different industrial environments and reducing dependency on extensive labeled datasets.

This book chapter presents a comprehensive study on the integration of FL and TL for distributed anomaly detection in IIoT-enabled power electronics. The research explores optimization techniques for scalable FL deployment, including low-latency model aggregation, edge-to-cloud collaboration, and privacy-preserving secure model aggregation using Secure Multi-Party Computation (SMPC). The role of meta-learning in improving FL model generalization for handling heterogeneous data was analyzed. To address computational inefficiencies, the study examines Federated Knowledge Distillation (FKD) as a lightweight learning approach that minimizes resource consumption while maintaining high anomaly detection accuracy. The findings highlight the advantages of hybrid FL-TL frameworks in enhancing fault diagnosis, reducing communication overhead, and ensuring energy-efficient real-time anomaly detection. The proposed approach strengthens the reliability and security of industrial automation by providing a scalable and adaptive learning framework for power electronics systems. Future research directions include optimizing FL-TL integration for dynamic industrial environments, developing energy-efficient federated architectures, and enhancing privacy-preserving techniques for large-scale IIoT networks.

Keywords: Federated Learning, Transfer Learning, Industrial IoT, Anomaly Detection, Secure Multi-Party Computation, Energy-Efficient Edge AI.

Introduction

The rapid expansion of the IIoT has significantly enhanced automation, predictive maintenance, and operational efficiency in power electronics [1]. Modern industrial systems rely on IIoT-enabled power electronic components, such as converters, inverters, and motor drives, to ensure energy efficiency and reliability [2]. The increasing complexity of these interconnected devices introduces challenges in detecting and mitigating anomalies that could lead to system failures, increased downtime, and operational inefficiencies [3,4]. Traditional anomaly detection models rely on centralized data processing, which poses critical challenges related to data privacy, high communication overhead, and computational inefficiencies. With the growing adoption of edge computing in industrial automation, there was a pressing need for decentralized learning approaches that enable real-time anomaly detection while preserving data privacy and optimizing resource utilization [5].

Federated Learning (FL) has emerged as a transformative paradigm that allows multiple edge devices to collaboratively train a global model without sharing raw data [6-9]. This decentralized approach ensures that sensitive industrial data remains localized, reducing security vulnerabilities while enabling continuous model updates across distributed systems. FL encounters several challenges, including communication constraints, non-independent and identically distributed (non-IID) data across edge devices, and the high computational costs associated with iterative model training [10]. These challenges hinder the effectiveness of FL-based anomaly detection in power electronics, necessitating the development of advanced optimization techniques to enhance model efficiency, adaptability, and scalability [11]. Addressing these limitations was crucial for enabling real-time fault diagnosis and predictive maintenance in IIoT-enabled industrial environments [12].

To further enhance the adaptability of FL models in heterogeneous industrial settings, Transfer Learning (TL) was integrated into FL frameworks to leverage pre-trained models and facilitate knowledge transfer across different operational environments [13]. TL enables FL models to generalize effectively in industrial power electronics applications by utilizing prior knowledge, reducing the need for extensive labeled datasets, and accelerating the learning process [14]. This approach was particularly beneficial in scenarios where collecting labeled anomaly data was impractical due to varying equipment configurations and environmental conditions. By incorporating TL, FL models can quickly adapt to new fault patterns, improving their accuracy and robustness across multiple IIoT-enabled industrial systems [15]. Additionally, TL reduces training costs and computational demands, making it a viable solution for resource-constrained edge devices deployed in industrial automation [16].

FL and TL, achieving scalability and computational efficiency in industrial automation remains a challenge. Techniques such as low-latency model aggregation, edge-to-cloud collaboration, and secure model aggregation using Secure Multi-Party Computation (SMPC) have been explored to optimize FL frameworks for large-scale IIoT applications [17]. Additionally, meta-learning has been introduced to enhance FL model generalization, allowing systems to adapt dynamically to changing industrial conditions [18-21]. Reducing computational overhead through Federated

Knowledge Distillation (FKD) was another critical area of research, where complex models are distilled into lightweight versions suitable for edge deployment without compromising anomaly detection accuracy. These advancements contribute to the development of more efficient and scalable federated frameworks for real-time fault diagnosis in industrial automation [22].

The integration of FL and TL provides a powerful framework for distributed anomaly detection in power electronics, addressing key challenges related to data privacy, computational efficiency, and model adaptability [23]. Future research should focus on refining hybrid FL-TL models, optimizing privacy-preserving techniques, and developing energy-efficient federated architectures for IIoT-enabled power electronics [24]. By leveraging these advancements, industrial automation systems can achieve higher resilience, reduced downtime, and improved predictive maintenance capabilities. Ensuring seamless integration of FL and TL in industrial environments drive the next generation of intelligent, self-adaptive, and privacy-preserving anomaly detection systems, contributing to the reliability and efficiency of modern power electronics applications [25].