RADemics

Time-Sensitive Networking (TSN) and 6G-Enabled Communication Frameworks for Low-Latency Control of IoT-Powered Industrial Power Electronics

S. Ram Prasath, M. Chiranjivi
KAMARAJ COLLEGE OF ENGINEERING AND TECHNOLOGY,
HYDERABAD INSTITUTE OF TECHNOLOGY AND MANAGEMENT

1. Time-Sensitive Networking (TSN) and 6G-Enabled Communication Frameworks for Low-Latency Control of IoT-Powered Industrial Power Electronics

[1]S. Ram Prasath, Assistant Professor, Department of Computer Science and Engineering, Kamaraj College of Engineering and Technology, Virudhunagar, Tamil Nadu, srpfxec@gmail.com

[2]M. Chiranjivi, Associate Professor, Department of Electrical and Electronics Engineering, Hyderabad Institute of Technology and Management, Telangana - 501401, chiranjivimadduluri@gmail.com

Abstract

The rapid integration of Internet of Things (IoT) and power electronics was revolutionizing modern smart grids and industrial automation, enabling intelligent control, real-time monitoring, and predictive maintenance. The seamless deployment of IoT-driven power electronic systems presents critical challenges related to communication interoperability, cybersecurity risks, data privacy, and real-time decision-making. This book chapter explores the role of advanced AI-driven analytics, edge computing, and blockchain-enabled security frameworks in enhancing the efficiency, reliability, and resilience of IoT-controlled power infrastructures. It presents an in-depth analysis of privacy-preserving data analytics, anomaly detection techniques, and interoperability solutions for heterogeneous IoT communication protocols in power electronics applications. The chapter investigates the application of Edge AI for real-time power system optimization, ensuring low-latency control and autonomous fault diagnosis. The discussion also highlights cybersecurity challenges and privacy-preserving mechanisms, including federated learning, differential privacy, and blockchain-based authentication, to mitigate data security risks in IoT-based power monitoring systems. By addressing key research gaps and presenting next-generation solutions for IoT-driven power electronics, this work provides a comprehensive framework for designing secure, intelligent, and high-performance energy systems.

Keywords: IoT-based power electronics, Smart grids, Edge AI, Privacy-preserving analytics, Cybersecurity, Real-time monitoring.

Introduction

The convergence of power electronics and the IoT has revolutionized modern smart grids and industrial automation by enabling real-time control, intelligent monitoring, and predictive analytics [1]. Traditional power electronic systems operated in isolated environments with minimal data exchange, but with the integration of IoT, these systems have evolved into interconnected networks capable of autonomous decision-making, adaptive energy management, and remote

diagnostics [2-5]. The proliferation of IoT-enabled sensors, intelligent controllers, and edge computing technologies has significantly enhanced the efficiency, flexibility, and resilience of power electronic infrastructures [6]. The transition to IoT-driven power electronics introduces numerous challenges related to interoperability, cybersecurity risks, data privacy, and latency constraints, which must be systematically addressed to ensure sustainable and secure operations [7].

One of the fundamental challenges in IoT-based power electronics was interoperability among diverse communication protocols and heterogeneous devices [8]. Power electronic systems operate in complex environments where multiple protocols, including MQTT, CoAP, OPC-UA, and DDS, facilitate data exchange across distributed networks. The lack of standardized frameworks for seamless communication between IoT-enabled power electronic devices leads to data silos, integration complexities, and inconsistent network performance [9,10]. To overcome these challenges, advanced solutions such as middleware-based interoperability, SDN, and AI-driven protocol optimization are being explored [11]. Ensuring reliable and secure data exchange among smart grids, industrial automation systems, and energy management platforms was crucial for maximizing the efficiency and scalability of IoT-integrated power electronics [12].

The increasing reliance on real-time data analytics and autonomous decision-making in power electronics further highlights the need for low-latency processing and computational efficiency [13]. Conventional cloud-based IoT architectures introduce delays in data transmission, high bandwidth consumption, and increased vulnerability to cyber threats, making them unsuitable for mission-critical applications. To address these limitations, Edge AI and federated learning have emerged as key enablers of intelligent, decentralized, and secure power electronics control [14]. Edge AI facilitates real-time anomaly detection, fault diagnosis, and predictive maintenance by processing data at the edge of the network, reducing reliance on centralized cloud infrastructure. This approach enhances response time, system reliability, and cybersecurity while ensuring that power electronic systems remain resilient against network failures and external threats [15-17].

Data privacy and cybersecurity remain significant concerns in IoT-based power electronics monitoring due to the increasing frequency of cyberattacks, data breaches, and unauthorized access [18]. Power electronic systems generate vast amounts of sensitive operational data, including load profiles, voltage fluctuations, and fault detection logs, which must be safeguarded against potential threats. Implementing privacy-preserving analytics techniques such as homomorphic encryption, differential privacy, and blockchain-based authentication ensures secure data processing while maintaining regulatory compliance with global data protection frameworks [19]. Additionally, zero-trust security architectures and AI-driven threat detection play a critical role in mitigating cybersecurity risks, preventing malicious intrusions, data tampering, and unauthorized system modifications [20].