RADemics

Federated Learning and Edge AI for Privacy Preserving Cybersecurity Models

Binu V P, Josephine Usha L, Deepthi K Bhasker
Govt Model Engineering College, SRM Institute of Science and Technology, Govt Model Engineering College

Federated Learning and Edge AI for Privacy Preserving Cybersecurity Models

[1]Binu V P, Associate Professor, Department of Computer Engineering, Govt Model Engineering College, Thrikakara Cochin-21,binuvp@mcc.ac.in.

[2]Josephine Usha L, Assistant Professor, School of Computing, SRM Institute of Science and Technology -Tiruchirappalli. josephineusha14@gmail.com

[3]Deepthi K Bhasker, Research Scholar, Department of Computer Engineering, Govt Model Engineering College, Thrikakara, Cochin-21, bh.deepthi@gmail.com

Abstract

The integration of Edge AI and Edge Computing represents a transformative paradigm in the field of cybersecurity, particularly in securing large-scale, decentralized IoT systems. As the number of connected devices continues to expand, traditional centralized security models struggle to provide real-time threat detection, low-latency responses, and data privacy. This chapter explores the synergies between Edge AI and Edge Computing, highlighting how localized intelligence and decentralized processing can enhance the security of remote and distributed systems. By enabling real-time anomaly detection, privacy-preserving data analysis, and rapid decision-making at the edge, these technologies offer significant advantages in preventing cyber threats across complex IoT ecosystems. The chapter delves into key aspects such as model optimization for resource-constrained devices, scalability in large networks, and the challenges posed by device heterogeneity and energy consumption. Furthermore, it emphasizes the role of machine learning, privacy-preserving techniques, and real-time threat mitigation in the deployment of Edge AI for cybersecurity. The potential of this combined approach is discussed with respect to its ability to improve the resilience and security of critical infrastructure, such as smart cities, industrial IoT, and autonomous systems. Ultimately, the chapter outlines the future directions and emerging research areas required to fully realize the capabilities of Edge AI and Edge Computing in next-generation cybersecurity frameworks.

Keywords: Edge AI, Edge Computing, IoT Systems, Cybersecurity, Machine Learning, Privacy-Preserving Techniques

Introduction

The digital landscape has evolved dramatically with the widespread adoption of Internet of Things (IoT) devices, which connect everyday objects to the internet, facilitating intelligent automation and data exchange [1]. From smart homes and healthcare devices to industrial IoT systems, the volume of data generated by these devices has reached unprecedented levels [2]. This explosion of data, coupled with the inherent vulnerabilities of IoT devices, presents significant challenges in terms of cybersecurity [3]. Traditional cloud-based security models are often ill-suited for managing the complexity, scale, and real-time requirements of modern IoT environments [4]. These systems are typically centralized, introducing latency due to data transmission and processing delays. To address these challenges, the convergence of Edge AI and Edge Computing offers a promising solution by bringing intelligence and processing capabilities closer to the devices generating the data, significantly enhancing the security and performance of IoT networks [5].

At its core, Edge Computing decentralizes data processing by moving computation and storage closer to the edge of the network, near the devices themselves [6]. This reduction in data travel distance not only reduces latency but also minimizes the potential for data breaches during transmission [7]. Edge Computing allows for real-time processing of data streams, enabling immediate detection of security threats and faster response times [8]. Coupled with Edge AI, which integrates machine learning algorithms at the device level, this architecture empowers IoT systems to autonomously analyze, detect, and mitigate potential threats without relying on centralized cloud infrastructure [9]. By processing data locally, Edge AI ensures that decisions are made instantaneously, enhancing the overall security posture of IoT systems by rapidly identifying anomalies, intrusions, or other suspicious activities [10].

The integration of Edge AI with Edge Computing creates a self-sustaining security framework that can operate even when devices are offline or disconnected from the cloud [11]. In traditional cloud-based systems, the need for continuous internet connectivity to send data to a central server often results in system vulnerabilities, especially in remote or resource-constrained environments [12]. This reliance on cloud infrastructure introduces the risk of latency and connectivity failure, which can lead to delayed detection and mitigation of cyber threats [13]. With Edge AI, data processing occurs locally, making the system more resilient to cyberattacks, such as Denial-of-Service (DoS) attacks, that aim to disrupt cloud communication channels [14]. Edge AI ensures data privacy by keeping sensitive information within local networks, addressing growing concerns over data security and compliance with privacy regulations, such as GDPR [15].