RADemics

Cybersecurity in IoT Ecosystems Using Lightweight Deep Learning Models

B. Padma Vijetha Dev, Kaliprasad C S, R. Kalpana
Gokaraju Rangaraju Institute of Engineering and Technology,
B. M. S. College Of Engineering, VISTAS.

Cybersecurity in IoT Ecosystems Using Lightweight Deep Learning Models

[1]B. Padma Vijetha Dev, Assistant Professor, CSE Department, Gokaraju Rangaraju Institute of Engineering and Technology, Bachupally Hyderabad. padmavijethadevb@gmail.com

[2]Kaliprasad C S, Assistant professor, physics, B. M. S. College Of Engineering, Bangalore-560019 India. Kpkaliprasadcs26@gmail.com

[3]R. Kalpana, Assistant professor, CSE-DS&IT, VISTAS Pallavaram Chennai. kalpana2002@gmail.com

Abstract

The rapid proliferation of Internet of Things (IoT) devices across diverse sectors has significantly increased the complexity of networked systems, introducing critical cybersecurity challenges. Traditional security mechanisms, reliant on centralized systems and static detection models, often fail to address the dynamic and decentralized nature of IoT environments. This chapter explores the integration of advanced machine learning techniques, particularly Federated Learning, and real-time collaborative threat detection for securing multi-tiered IoT ecosystems. Emphasizing low-latency decision-making, this work highlights the importance of distributed, real-time threat sharing and coordination across IoT devices, edge systems, and cloud infrastructures. By leveraging Federated Learning for decentralized model training, the chapter offers solutions for privacy-preserving, scalable, and adaptive threat detection and response. Moreover, it delves into the optimization of detection models for low-latency applications, ensuring prompt and effective responses to emerging cyber threats. Challenges such as device heterogeneity, data sparsity, and communication overhead are examined, with a focus on practical strategies for addressing these issues. This chapter ultimately provides a comprehensive framework for enhancing IoT security through collaborative, real-time, and decentralized approaches, paving the way for future research in adaptive security architectures.

Keywords: IoT Security, Federated Learning, Real-Time Threat Detection, Low-Latency Decision-Making, Distributed Systems, Privacy-Preserving Models.

Introduction

The rise of the Internet of Things (IoT) has revolutionized industries by enabling seamless communication and real-time data exchange across a multitude of devices [1]. As IoT systems expand, they create vast, interconnected networks that bring significant benefits, including enhanced automation, improved operational efficiency, and real-time monitoring [2]. However, this rapid proliferation of connected devices has also introduced new and complex cybersecurity challenges [3]. Traditional security models, designed for centralized systems, struggle to adapt to the decentralized nature of IoT networks. Each IoT device represents a potential entry point for cyberattacks, which can lead to data breaches, system disruptions, and even physical damage in critical infrastructure settings [4]. To address these risks, there is a growing need for advanced security mechanisms capable of providing real-time threat detection and response within these dynamic, distributed networks [5].

At the core of IoT security lies the challenge of detecting and mitigating threats in real time [6]. The highly dynamic nature of IoT environments where devices constantly communicate, generate data, and adapt to changing conditions requires a security framework that can quickly identify anomalous behaviors and respond accordingly [7]. Traditional signature-based approaches, which rely on predefined patterns of attack, are insufficient for identifying novel threats that may not yet have been encountered [8]. To overcome this limitation, machine learning (ML) models have been employed for their ability to detect complex patterns and adapt to new, unseen threats [9]. However, the computational demands of such models can be a barrier, especially for resource-constrained IoT devices, which often lack the processing power required to handle large datasets or execute complex algorithms efficiently. This challenge underscores the importance of developing more lightweight and adaptive models tailored for IoT security [10].

Federated Learning (FL) has emerged as a promising solution to address these challenges in the context of IoT cybersecurity [11]. FL is a decentralized machine learning technique that enables multiple devices to collaboratively train a model without sharing their raw data [12]. In this approach, each IoT device trains a local model based on its own data and then shares only the model updates with a central server. The server aggregates these updates to improve a global model, which is then redistributed to participating devices [13]. This process preserves data privacy and significantly reduces the communication overhead, which is especially critical in environments where IoT devices are numerous and often operate in resource-constrained conditions [14]. By leveraging FL, IoT networks can achieve scalable and privacy-preserving security solutions that continuously improve over time, as each device contributes to the global model based on its real-time observations [15].