RADemics

Hybrid Deep Learning Architectures for Scalable Security in IoT and Edge Computing Environments

V.Samuthira Pandi , Shobana D , Prabhu V
Chennai Institute of Technology, Rajalakshmi Engineering College, R.M.K. Engineering College.

16. Hybrid Deep Learning Architectures for Scalable Security in IoT and Edge Computing Environments

1V.Samuthira Pandi, Department of ECE, Centre for Advanced Wireless Integrated Technology,
Chennai Institute of Technology, Chennai. samuthirapandiv@citchennai.net

2Shobana D ,Department of Mechatronics.Rajalakshmi Engineering College, shobana.d@rajalakshmi.edu.in

3Prabhu V, Associate Professor, Department of Computer Science and Engineering, R.M.K. Engineering College, RSM Nagar, Kavaraipettai, Gummidipoondi(Taluk), Thiruvallur(District), Tamil Nadu, India,Pincode - 601206.pbv.cse@rmkec.ac.in

Abstract

The proliferation of Internet of Things (IoT) and edge computing technologies has transformed digital ecosystems, enabling real-time data processing and intelligent decision-making. The massive interconnectivity and resource-constrained nature of these devices expose them to sophisticated cyber threats, including data breaches, adversarial attacks, and malware intrusions. Traditional security mechanisms fail to provide adaptive and scalable protection against these evolving threats. Recent advancements in deep learning (DL) have demonstrated significant potential in enhancing cybersecurity through automated threat detection and anomaly identification. Standalone DL models often suffer from limitations such as high computational overhead, vulnerability to adversarial attacks, and poor generalization in dynamic environments. This chapter presents a hybrid deep learning architecture designed to enhance the security and scalability of IoT and edge computing environments. The proposed framework integrates convolutional neural networks (CNNs) for feature extraction and recurrent neural networks (RNNs) for sequential pattern recognition, ensuring robust anomaly detection while maintaining computational efficiency. Additionally, attention mechanisms and federated learning approaches are incorporated to improve adaptability and resilience against emerging cyber threats. Experimental evaluations demonstrate that the hybrid model achieves superior accuracy, lower false positive rates, and enhanced real-time performance compared to conventional security frameworks. This study provides critical insights into optimizing hybrid deep learning models for large-scale deployment in IoT and edge networks, addressing challenges related to resource constraints, data privacy, and adversarial robustness. Future research directions are outlined to further improve the efficiency, interpretability, and security of deep learning-based intrusion detection systems.

Keywords: Hybrid Deep Learning, IoT Security, Edge Computing, Anomaly Detection, Federated Learning, Cyber Threats.

Introduction

The rapid expansion of the Internet of Things (IoT) and edge computing has revolutionized modern technological landscapes by enabling real-time data processing, autonomous decision-making, and seamless communication between interconnected devices [1]. These advancements have significantly impacted industries such as healthcare, smart cities, industrial automation, and intelligent transportation systems [2]. IoT and edge computing reduce reliance on centralized cloud infrastructure, allowing data to be processed closer to its source, thereby minimizing latency and enhancing operational efficiency [3]. This decentralized nature also introduces substantial security vulnerabilities, as edge devices often operate in resource-constrained environments with limited computational power and security provisions [4]. The increasing sophistication of cyber threats, including data breaches, adversarial attacks, and malware intrusions, has created an urgent need for robust and scalable security mechanisms capable of protecting IoT networks from evolving threats [5].

Traditional security approaches, such as rule-based intrusion detection systems (IDS) and conventional cryptographic techniques, have proven inadequate in addressing the complex and dynamic security challenges faced by IoT and edge computing systems [6]. These methods often struggle to adapt to novel attack patterns and suffer from high false-positive rates, making them inefficient for large-scale deployment [7]. The computational overhead associated with traditional security mechanisms makes them unsuitable for resource-limited edge devices [8]. To overcome these limitations, machine learning and deep learning-based security frameworks have gained significant attention due to their ability to detect and classify cyber threats with high accuracy [9]. Deep learning models can automatically extract features from vast amounts of network traffic data, enabling proactive threat detection without requiring manual intervention [10].

While deep learning has shown promising results in cybersecurity applications, standalone deep learning models encounter several limitations that hinder their deployment in real-world IoT environments [11]. One of the primary challenges was the high computational cost associated with training and inference, making it difficult to implement deep learning-based security models on edge devices with constrained processing power [12]. Additionally, deep learning models are highly susceptible to adversarial attacks, where small perturbations in input data can cause significant misclassifications, rendering the models ineffective against sophisticated cyber threats [13]. The lack of interpretability in deep learning models further complicates their deployment, as security analysts often struggle to understand the reasoning behind anomaly detection decisions, making it challenging to fine-tune models for enhanced performance [14].

Hybrid deep learning architectures have emerged as a potential solution, combining multiple deep learning models to leverage their respective strengths while mitigating their weaknesses [15]. Convolutional neural networks (CNNs) are highly effective at extracting spatial features from network traffic data, whereas recurrent neural networks (RNNs) and Long Short-

Term Memory (LSTM) networks are capable of capturing sequential dependencies, making them suitable for detecting patterns in time-series data [16]. By integrating CNNs and RNNs, hybrid architectures can enhance anomaly detection capabilities while maintaining computational efficiency [17]. Additionally, federated learning and attention mechanisms further improve the adaptability and scalability of hybrid deep learning models, enabling secure and privacy-preserving threat detection in distributed IoT environments [18].

This explores the development and implementation of hybrid deep learning-based security frameworks for IoT and edge computing environments [19]. The proposed architecture integrates multiple deep learning models to improve the accuracy, efficiency, and resilience of intrusion detection systems [20]. Through experimental evaluations, the effectiveness of the hybrid approach was analyzed, demonstrating its ability to detect complex cyber threats with minimal false positives [21]. The associated with deploying deep learning-based security solutions in resource-constrained environments and proposes optimization techniques to enhance real-time threat detection capabilities [22-25].