RADemics

AI-Driven Secure Communication and Anomaly Detection in 5G-Connected IoT Power Electronics Networks

Ramesh Bharti , Sowmitha V
Faculty of Engineering & Technology,
K S R College of Engineering

12. AI-Driven Secure Communication and Anomaly Detection in 5G-Connected IoT Power Electronics Networks

[1]Ramesh Bharti, Professor, Department of Electronics & Communication Engineering, Faculty of Engineering & Technology, Jagannath University, Jaipur, Rajasthan, India. er.rbharti@gmail.com

[2]Sowmitha V, Assistant Professor, Department of Computer Science and Engineering, K S R College of Engineering, Tiruchengode, Tamil Nadu, India, sowmitha002@gmail.com

Abstract

The rapid proliferation of 5G-enabled IoT networks has significantly increased cybersecurity vulnerabilities, necessitating the development of advanced intrusion detection mechanisms. Traditional security solutions struggle to address the dynamic and complex nature of cyber threats targeting resource-constrained IoT devices. To overcome these challenges, the integration of AI and blockchain technology presents a novel approach to enhancing real-time intrusion detection and threat mitigation. AI-driven intrusion detection systems (IDS) leverage deep learning and machine learning models to analyze network anomalies, while blockchain ensures data integrity, decentralization, and tamper resistance. The implementation of AI-Blockchain IDS faces critical challenges, including scalability, computational overhead, interoperability, and adaptability to evolving cyber threats. This book chapter explores the convergence of AI and blockchain for secure intrusion detection in 5G-IoT environments, addressing key challenges, deployment strategies, and future research directions. The discussion highlights the role of Edge AI in enabling real-time threat detection for resource-constrained IoT devices and examines the potential of federated learning for decentralized security. Additionally, transfer learning techniques are explored to enhance the adaptability of deep learning-based IDS. Case studies on Edge AI-powered IDS deployment in smart grids, healthcare, and industrial IoT networks demonstrate the effectiveness of these technologies in mitigating cyber risks. The chapter also presents a comparative analysis of various machine learning algorithms for intrusion detection, evaluating their efficiency in securing 5G-IoT infrastructures. By addressing existing research gaps and proposing innovative solutions, this work contributes to the advancement of AI-driven secure communication and anomaly detection frameworks in next-generation IoT networks.

Keywords: Intrusion Detection, AI-Blockchain Security, 5G-IoT, Edge AI, Federated Learning, Cyber Threats.

Introduction

The rapid deployment of 5G-enabled IoT networks has transformed modern communication systems, offering ultra-low latency, massive device connectivity, and high-speed data transmission [1,2]. These advancements have enabled critical applications such as smart cities, industrial

automation, healthcare monitoring, and autonomous transportation systems [3]. IoT devices continue to proliferate across interconnected environments, the attack surface for cyber threats has expanded exponentially [4]. Security breaches, unauthorized data access, and network intrusions have become significant concerns, threatening the confidentiality, integrity, and availability of sensitive information. Traditional security mechanisms, such as firewalls and signature-based intrusion detection systems (IDS), struggle to provide adequate protection due to the heterogeneous nature of IoT devices and the dynamic nature of cyberattacks [5]. Consequently, there was a growing need for intelligent and adaptive security solutions capable of mitigating emerging threats in real time [6].

AI has emerged as a promising approach to enhance intrusion detection in complex 5G-IoT environments [7]. AI-driven IDS leverage machine learning and deep learning techniques to analyze vast amounts of network traffic data, detect anomalies, and identify malicious activities with high accuracy. Unlike rule-based IDS, AI models continuously learn from evolving attack patterns, enabling proactive threat detection without extensive manual intervention [8]. Deep learning architectures, such as CNNs and recurrent neural networks (RNNs), enhance IDS capabilities by extracting high-dimensional features from network behavior. The integration of AI in intrusion detection was not without challenges [9,10]. The computational demands of deep learning models, adversarial attacks on AI algorithms, and data privacy concerns pose significant barriers to large-scale adoption [11]. Optimizing AI-driven IDS for real-time security monitoring requires innovative approaches that balance accuracy, efficiency, and resource utilization, particularly in constrained IoT environments [12].

Blockchain technology has gained attention as a complementary security solution that enhances intrusion detection frameworks by ensuring data integrity, decentralization, and transparency [13]. Traditional IDS often rely on centralized architectures, making them vulnerable to single points of failure and data tampering [14]. By leveraging blockchain, security mechanisms can store network activity logs in immutable distributed ledgers, preventing unauthorized modifications and ensuring accountability. Smart contracts enable automated intrusion response mechanisms, where predefined security policies are executed without human intervention. Additionally, consensus mechanisms validate anomaly detection reports, reducing false positives and improving trustworthiness in collaborative intrusion detection environments [15-17]. Despite these advantages, blockchain-based IDS implementation faces challenges such as high computational overhead, scalability limitations, and latency issues in real-time detection. Addressing these constraints requires the development of lightweight consensus algorithms and efficient blockchain architectures tailored for resource-limited IoT devices [18].

Edge AI has emerged as a critical enabler for real-time intrusion detection in 5G-IoT ecosystems, particularly for resource-constrained devices that cannot afford frequent cloud communication. Traditional cloud-based security solutions suffer from latency and bandwidth limitations, making them less effective for real-time threat mitigation [19]. Edge AI-driven IDS processes security events closer to the data source, reducing dependency on centralized servers while enabling faster threat response. Federated learning further enhances this approach by enabling distributed IoT nodes to collaboratively train IDS models without exposing raw data, preserving privacy and reducing network congestion [20]. Additionally, transfer learning techniques allow pre-trained IDS models to be adapted for new attack patterns, reducing the computational burden of model training. Deploying AI-driven IDS at the edge introduces challenges related to energy efficiency, model optimization, and the trade-off between detection

accuracy and computational complexity [21]. Future research must focus on designing lightweight deep learning models that balance security effectiveness with the constrained processing capabilities of edge devices.

This book chapter presents a comprehensive analysis of AI-driven and blockchain-enhanced intrusion detection frameworks for securing 5G-enabled IoT networks [22]. It explores the challenges of implementing AI-powered IDS in real-time security environments and investigates the role of blockchain in strengthening intrusion detection mechanisms [23]. Additionally, the study examines Edge AI-driven IDS deployments, focusing on their effectiveness in mitigating cyber threats for smart grids, healthcare systems, industrial IoT, and autonomous transportation networks [24]. A comparative evaluation of machine learning algorithms for intrusion detection was also conducted, highlighting their strengths and limitations in securing 5G-IoT infrastructures. By addressing existing research gaps, this work aims to contribute to the development of next-generation security frameworks that integrate AI, blockchain, and edge computing to enhance intrusion detection and threat mitigation in future IoT ecosystems [25].