RADemics

# Application of Federated Learning Models for Privacy-Preserving Detection of Cyber Attacks in Cross-Domain Networks

P. Krishnamoorthy, R. Menaka
SASI INSTITUTE OF TECHNOLOGY & ENGINEERING,
VELALAR COLLEGE OF ENGINEERING AND TECHNOLOGY

# Application of Federated Learning Models for Privacy-Preserving Detection of Cyber Attacks in Cross-Domain Networks

[1]P. Krishnamoorthy, Associate Professor, Department of Computer Science and Engineering, Sasi Institute of Technology & Engineering, Tadepalligudem, West Godavari District, Andhra Pradesh, India. krishnancse0206@gmail.com

[2]R. Menaka, Assistant Professor, Department of Information Technology, Velalar College of Engineering and Technology, Thindal, Erode, Tamil Nadu, India. menakavcet@gmail.com

## Abstract

This book chapter explores the integration of Federated Learning (FL) with cybersecurity, focusing on its potential to enhance privacy-preserving detection of cyberattacks in cross-domain networks. As cyber threats evolve in complexity and scale, traditional centralized approaches face limitations in terms of data privacy and scalability. FL offers a decentralized framework where local models are trained on distributed data, ensuring privacy while enabling real-time threat detection. This chapter delves into the core concepts of FL, its relevance to cybersecurity, and its application in mitigating cyber risks across mobile, edge, and IoT devices. Key topics include improving model accuracy, reducing false positives, and integrating FL with advanced threat intelligence platforms for proactive defense. Challenges such as scalability, communication overhead, and the integration of diverse security techniques are discussed. The chapter provides insights into how FL can revolutionize modern cybersecurity frameworks, ensuring robust and adaptive defense mechanisms in complex digital environments.

**Keywords:** Federated Learning, Cybersecurity, Privacy-Preserving, Threat Detection, Cross-Domain Networks, IoT Security

## Introduction

Federated Learning (FL) has emerged as a transformative approach in machine learning, particularly in addressing the growing concerns around privacy, scalability, and data security [1-3]. In the context of cybersecurity, FL offers a decentralized method for training models without the need for centralizing sensitive data [4]. This was especially crucial as the volume of data generated across various domains, including IoT devices, mobile networks, and edge computing, continues to expand [5]. Traditional cybersecurity systems, which rely on centralized data collection and model training, often face significant privacy risks and inefficiencies when handling sensitive information [6]. Federated Learning mitigates these concerns by allowing individual devices or nodes to train local models on their data, while only sharing aggregated updates with a central server [7,8]. This approach significantly reduces the risk of data breaches and privacy violations, making it a critical technology for privacy-preserving cybersecurity [9,10].

The main advantage of Federated Learning in cybersecurity lies in its ability to enhance privacy without sacrificing model accuracy or performance [11,12]. In conventional machine learning systems, centralized data storage often leads to data aggregation challenges and vulnerabilities [13,14]. By decentralizing the learning process, FL ensures that data remains local, and only model parameters are exchanged, protecting user privacy [15-18]. FL allows for continuous learning and real-time updates, which was essential in detecting emerging cyber threats [19]. This was particularly important in dynamic environments where cyberattack techniques evolve rapidly, and traditional models struggle to keep up [20]. FL enables faster adaptation to new threats, as local devices can quickly incorporate new information without waiting for central updates [21]. Thus, Federated Learning provides a robust solution to evolving security challenges while maintaining compliance with stringent privacy regulations such as GDPR [22].

The application of Federated Learning in cross-domain networks brings additional complexity, but also greater potential for enhancing cybersecurity [23,24]. Cross-domain networks are characterized by the interaction of multiple, diverse devices and platforms across various industries, including healthcare, finance, and critical infrastructure. These networks often involve different types of data, protocols, and security needs, which makes it challenging to implement uniform cybersecurity measures [25]. FL can help overcome these challenges by enabling the creation of cross-domain models that learn from diverse datasets without the need for centralized data storage. Each domain can contribute to a global model, improving threat detection and mitigation across all connected networks. This ability to learn from a broad range of data sources while ensuring privacy and security was what makes Federated Learning a promising approach for cybersecurity in highly interconnected, cross-domain environments.