RADemics

Federated Learning for Distributed Threat Intelligence Sharing Across Global Cybersecurity Networks

Sowmiya S M, Nachimuthu S, A. Narayana Rao
VELS INSTITUTE OF SCIENCE, TECHNOLOGY AND ADVANCED STUDIES, VELALAR COLLEGE OF ENGINEERING AND TECHNOLOGY, NBKRIST (Autonomous),

Federated Learning for Distributed Threat Intelligence Sharing Across Global Cybersecurity Networks

[1]Sowmiya S M, Assistant Professor, Computer Science and Engineering, Vels institute of Science, Technology and Advanced Studies, Krishnapuram, Pallavaram, Chennai-600117, Tamilnadu, smsowmiya.se@vistas.ac.in

[2]Nachimuthu S, AP ECE, Velalar College of Engineering and Technology, Erode, nachi.velalar@gmail.com

[3]A. Narayana Rao, Professor & HOD, Department of IT and AI&DS, NBKRIST (Autonomous), Vidyanagar, Gudur, Tirupati-524413.narayanaraoappini@gmail.com

Abstract

The rapid evolution of cyber threats necessitates innovative approaches to enhance global cybersecurity collaboration. Federated Learning (FL) has emerged as a decentralized machine learning paradigm that enables distributed threat intelligence sharing while maintaining data privacy and security. This chapter explores the application of FL for large-scale cybersecurity networks, addressing critical challenges in scalability, security, and communication efficiency. The focus is on optimizing secure aggregation techniques to enable efficient and privacy-preserving model updates across heterogeneous and resource-constrained environments. Key solutions such as hierarchical aggregation, sparse model updates, and blockchain-based enhancements are discussed to mitigate the computational and communication overheads inherent in federated systems. the chapter investigates the integration of advanced cryptographic methods, including homomorphic encryption and differential privacy, to strengthen the security of federated networks against adversarial attacks. By leveraging FL's potential, organizations can share threat intelligence across global networks without compromising sensitive data, significantly improving real-time cyber threat detection and response. The chapter concludes by identifying future research directions for overcoming existing challenges and further optimizing federated models in cybersecurity.

Keywords: Federated Learning, Cybersecurity, Secure Aggregation, Threat Intelligence Sharing, Blockchain, Privacy-Preserving Models.

Introduction

The rapid escalation of cyber threats across the globe has transformed cybersecurity into an urgent and ongoing priority for governments, businesses, and individuals. Traditional cybersecurity defense mechanisms, such as firewalls, intrusion detection systems, and antivirus software, are often unable to keep up with the sophistication and evolving nature of cyberattacks. Attackers are becoming increasingly adept at evading detection and exploiting vulnerabilities across diverse, interconnected digital infrastructures. To combat these threats, it has become crucial for organizations to collaborate in sharing threat intelligence, which includes valuable data

on attack vectors, tactics, techniques, and procedures (TTPs) used by adversaries. However, traditional methods of centralized data sharing often encounter significant challenges related to data privacy, regulatory constraints, and the risks associated with a single point of failure. Federated Learning (FL) offers a novel decentralized solution that enables collaborative machine learning model training while ensuring the confidentiality and privacy of the data shared across participants.

Federated Learning (FL) is a machine learning paradigm that allows multiple participants (such as organizations or security entities) to collaboratively train a model without sharing raw data. Instead of pooling data into a central repository, each participant trains a local model on their own data and then shares only the model updates (i.e., weights and gradients) with a central server. This decentralized approach ensures that sensitive information remains within the local domain, providing an inherent layer of privacy preservation. FL has shown great promise in a variety of domains, such as healthcare, finance, and mobile applications, where privacy is a significant concern. In the context of cybersecurity, FL offers an innovative solution to the growing demand for cross-organization threat intelligence sharing while mitigating the risks associated with exposing sensitive security data. By enabling organizations to share threat intelligence without compromising data privacy, FL can contribute to the collective defense against cyber adversaries, enhancing the overall resilience of the global cybersecurity ecosystem.

While the potential benefits of Federated Learning in distributed threat intelligence sharing are clear, significant challenges remain when deploying FL on a global scale. One of the primary concerns is scalability, particularly when the number of participants in a federated network increases. As the size of the network grows, the frequency of model updates and communication between participants also rises, leading to increased computational and bandwidth requirements. Large-scale FL deployments in cybersecurity face several hurdles, including the difficulty of securely aggregating model updates from a diverse range of participants. The aggregation process must be efficient to ensure that the model converges in a reasonable time frame, especially in real-time cybersecurity applications where the speed of threat detection is critical. resource-constrained devices, such as Internet of Things (IoT) devices, mobile endpoints, and edge computing nodes, often struggle with the computational complexity required for training and updating FL models, which can hamper the scalability of federated systems in real-world environments.

One of the most significant challenges in implementing FL for cybersecurity is the need for secure aggregation of model updates. In a federated network, participants send their model updates to a central server for aggregation. However, without proper security measures, these updates can be vulnerable to malicious attacks, such as model poisoning, where an adversary manipulates their local model updates to compromise the global model. Secure aggregation ensures that only the aggregated model updates are shared, without revealing individual updates that could potentially contain sensitive or manipulated information. Several cryptographic techniques, such as homomorphic encryption, secure multi-party computation (SMPC), and differential privacy, are commonly used to secure model updates during aggregation. However, as federated networks scale, the computational and communication overhead of these techniques increases, making it challenging to maintain efficiency and security in large-scale deployments. The need for scalable and secure aggregation techniques that minimize both communication and computational costs while ensuring data privacy and integrity is paramount in realizing the full potential of FL in cybersecurity applications.