

Developing a privacy-preserving federated learning framework for intrusion detection in IoT networks using ethical hacking simulations

Raaziya M.Z.H.F.^{1*}, Abeythunga W.M.L.S.²

¹Department of Computing and Information Systems,
Faculty of Computing, Sabaragamuwa University of Sri Lanka

²Department of Software Engineering,
Faculty of Computing, Sabaragamuwa University of Sri Lanka

*raziamzh@gmail.com

The Internet of Things has transformed modern systems by integrating artificial intelligence, cybersecurity, and real-time analytics into billions of interconnected devices. However, decentralization and resource constrained IoT networks are vulnerable to cyberattacks such as Distributed Denial-of-Service and data poisoning. Conventional centralized intrusion detection systems require the transmission of raw data to a central server, which violates privacy regulations such as GDPR and introduces single points of failure. Existing federated learning (FL) approaches for IoT IDS employ differential privacy, homomorphic encryption, or blockchain on static, such studies are mainly based on offline assessments and do not include the simulation of real-time ethical hacking against dynamic threats. This research addresses this gap by proposing a privacy-protecting FL system based on Federated Averaging. A binary classification model was trained, with an accuracy of 89%. A simulation of ethical hacking was performed on hping3 to generate a live SYN flood attack, which produced malicious packets that were captured under the use of tcpdump and verified in Wireshark. The framework was able to identify most attack packets, and this indicates it has robust real-time performance. The framework mitigates privacy risks in centralized systems and shows scalability for resource constrained devices. Limitations include reliance on simulated rather than physical IoT devices and evaluation focused primarily on DoS attacks.

Keywords: *Federated Learning; Intrusion Detection System; Internet of Things; Ethical Hacking; Simulation*