Chapter 12
Revolutionizing Network Security Stacked Generalization for Malicious Traffic Detection

Harsh Jain
https://orcid.org/0009-0004-5752-3029
SRM Institute of Science and Technology, Ramapuram, India

Suhas Srinivas Lingam
https://orcid.org/0009-0001-0205-0728
SRM Universtiy, India

Azhagiri Mahendiran
https://orcid.org/0000-0002-6124-3773
SRM Institute of Science and Technology, Ramapuram, India

Karthik Srinivasan
https://orcid.org/0000-0002-9822-2060
Saudi Electronic University, Saudi Arabia

ABSTRACT

The rising complexity of cyberattacks challenges traditional network security systems. To address this, we propose a layered generalization approach using multiple machine learning classifiers and XGBoost as a meta-learner to detect malicious network traffic more effectively. Stacking enhances prediction accuracy by combining base model strengths and reducing weaknesses. The classifiers are trained

DOI: 10.4018/979-8-3373-3541-4.ch012

on real-world network traffic features, with XGBoost aggregating their outputs to improve detection. Its scalability, efficiency, and handling of imbalanced data suit real-world traffic's benign-malicious imbalance. Experiments on the CIC-IDS2017 dataset show that our stacked framework outperforms individual models in accuracy, precision, recall, and F1-score, significantly reducing false positives and negatives while strengthening network protection.

INTRODUCTION

Let's be real: the digital revolution didn't just tweak modern life; it basically flipped the whole thing on its head. Governments, businesses, even your grandma's knitting club—everyone's tangled up in these insanely complex digital networks now. So yeah, keeping that infrastructure locked down? Kinda a big deal. You've got Zang and crew (2024) pointing out how cyberattacks aren't just annoying anymore—they're nastier, sneakier, and popping up all the freaking time. Makes you wonder if hackers ever sleep. All this means network securities got some serious holes, and let's be honest, it's stressing out the folks who have to patch them (Suriyan et al., 2026; Xue et al., 2024). Then there's Ahmed et al. (2025) jumping in, basically saying forget about that one-off hacker in his mom's basement. Now we're talking about non-stop, always-on threats. Sensitive data? At risk. Uptime? Good luck. Company reputation? On the line, 24/7. No wonder IT and security pros are sweating bullets—these attacks are relentless, and it's like playing whack-a-mole but with way higher stakes.

Among the most important dangers, DDOS attacks, advanced continuous Threatening, phishing campaign, ransomware, botnets, and other advanced malware strains. These attacks exploit the dynamic and odd nature of the modern network, making traditional signature-based and rules-based security solutions rapidly ineffective (Sidharth & Kavitha, 2021). Traditional intrusion Systems (IDs) and firewalls greatly rely on predetermined patterns and approximation rules to detect malicious activities. Effective against known dangers, these systems fail to detect novel and sophisticated attacks, especially zero-day weaknesses and polymorphic malware, where no pre-signature is present (Mills et al., 2024; Singh and Dubey, 2015, Singh and Kaushik, 2023a; Singh and Kaushik, 2023b).

In response to the insufficiency of traditional systems, machine learning evolved as a promising solution to increase network security. By analyzing patterns in network traffic and identifying the deviation of malicious behavior, the ML algorithm introduced a dynamic and active approach to detect the danger (Pubudu et al., 2021). For identifying infiltration and network flows, decisions have shown crucial involvement in classification (Ali et al., 2023). Meanwhile real-world standalone machine