ABSTRACT

Meningkatnya keragaman dan kompleksitas infrastruktur jaringan telah membuat pendeteksian serangan Distributed Denial-of-Service (DDoS) semakin sulit, terutama dalam lingkungan heterogen. Metode deteksi tradisional sering kali kesulitan mempertahankan kinerja tinggi di berbagai kondisi jaringan. Namun, studi ini mengatasi masalah tersebut dengan mengusulkan Collaborative Intrusion Detection System (CIDS) yang memanfaatkan penumpukan ensemble dari beberapa model pembelajaran mendalam untuk meningkatkan generalisasi dan akurasi deteksi. Kerangka kerja ini menggabungkan beberapa jaringan saraf dalam sebagai pembelajar dasar, dengan meta-pembelajar yang mengintegrasikan keluarannya untuk prediksi akhir. Evaluasi dilakukan menggunakan tiga set data berbasis NetFlow—NF-ToN-IoT, NF-BoT-IoT, dan NF-CSE-CIC-IDS2018—yang masing-masing mewakili status jaringan yang berbeda. Metode yang diusulkan mencapai akurasi puncak sebesar 84,7%, yang menunjukkan bahwa pendekatan penumpukan ensemble secara signifikan meningkatkan kemampuan deteksi DDoS dalam lingkungan jaringan yang kolaboratif dan heterogen.