ABSTRAK

Proliferasi perangkat IoT yang meluas telah menyebabkan peningkatan besar dalam serangan DDoS berbasis IoT, yang menimbulkan ancaman kritis bagi jaringan rumah pintar dan ekosistem lain yang terhubung dengan IoT. Solusi keamanan yang ada tidak mampu mengidentifikasi varian malware IoT yang baru dan canggih secara efektif. Makalah ini menyajikan pendekatan berbasis pembelajaran mesin menggunakan pengklasifikasi K-Nearest Neighbor (KNN) dan varian ensemble Bagging-nya untuk mengidentifikasi beragam serangan DDoS seperti SYN Flood, UDP Flood, dan varian botnet Mirai dalam lalu lintas jaringan IoT. Dalam penelitian ini, dataset CICIoT2023 dan metode pemilihan fitur berbasis korelasi digunakan untuk mengidentifikasi atribut yang paling berpengaruh untuk mengkategorikan serangan. Eksperimen menunjukkan bahwa model KNN dasar mencapai akurasi, presisi, recall, dan skor F1 yang luar biasa, lebih dari 97%, dengan overhead komputasi yang lebih rendah dibandingkan dengan pendekatan ensemble, sehingga dapat diterapkan secara real-time di lingkungan IoT dengan sumber daya rendah. Artikel ini mendemonstrasikan kelayakan model pembelajaran mesin ringan untuk mewujudkan deteksi intrusi yang efektif dan efisien dalam jaringan IoT rumah pintar. Penelitian selanjutnya akan mengeksplorasi rekayasa fitur yang lebih kompleks dan kerangka kerja pembelajaran ensemble untuk meningkatkan deteksi perilaku serangan baru.

Kata Kunci: Distributed Denial of Service, Botnet IoT, Machine Learning, K-Nearest Neighbor, Smart Home Security