ABSTRAK

Kemajuan teknologi jaringan telah mendorong segalanya hingga ke batasnya, meningkatkan produktivitas di hampir semua sektor industri yang ada. Namun, manfaat tersebut juga membawa risiko. Dengan tingkat keterhubungan dunia yang sangat tinggi, serangan diam-diam terhadap jaringan mulai bermunculan. Untuk menangkal serangan-serangan ini, sebuah jaringan harus dilengkapi dengan berbagai lapisan perlindungan, salah satunya adalah *Intrusion Detection System* (IDS).

IDS melindungi jaringan secara pasif dengan membandingkan paket yang masuk dengan *signature* serangan yang telah diketahui. Sistem tradisional berbasis database berisi *signature* serangan telah terbukti efektif, namun dengan bentuk serangan yang terus berubah, dibutuhkan penerapan tambahan kecerdasan buatan (*Artificial Intelligence* / AI) untuk membantu mendeteksi serangan baru yang belum terdokumentasi.

IDS berbasis AI telah ada sejak lama, dengan berbagai penelitian yang mencakup metode *Machine Learning* (ML) hingga *Deep Learning* (DL). Namun, model DL yang lebih canggih seperti *Convolutional Neural Network* (CNN) memiliki kelemahan konseptual ketika digunakan untuk dataset berbentuk tabular, yang pada kenyataannya menjadi format umum hampir semua dataset intrusi. Selain itu, banyak penelitian mengabaikan konsep generalisasi antar lingkungan yang bersifat penting dan juga krusial bagi solusi IDS yang dapat diterapkan secara luas.

Di sinilah TabNet hadir. Dalam penelitian ini, TabNet digunakan untuk membangun model yang dapat melakukan generalisasi pada dua jenis dataset: *impact-based* dataset dan *lifecycle-based* dataset. Dataset *impact-based* terdiri dari CIC-IDS-2017 dan CIC-IDS-2018, sedangkan dataset *lifecycle-based* terdiri dari CREMEv1 dan CREMEv2. Dengan melakukan pengujian silang di antara semua dataset, hasil yang diperoleh sangat mengesankan, dengan rentang kinerja F1-Score yang secara umum tinggi, yakni 82% hingga 99%, dibandingkan XGBoost yang memiliki rentang kinerja lebih bervariasi, yakni 22% hingga 99% pada skenario generalisasi *binary* maupun *multiclass*.

Keywords: *Deep Learning*, *Intrusion Detection System*, Keamanan Jaringan, TabNet