

ABSTRAK

Penggunaan teknologi dalam pendeteksian serangan jaringan merupakan salah satu ide solusi yang efisien, untuk mengamankan sistem komputer. CIDS merupakan sistem monitoring lalu lintas jaringan yang dirancang untuk mendeteksi jenis serangan, CIDS terdiri dari beberapa komponen yang terdistribusi di masing-masing node jaringan, penelitian berfokus pada pembuatan model *deep neural network* dan *federated learning* pada sistem CIDS, dimana kumpulan data mampu dilatih dengan cara desentralisasi tanpa harus mengirimkan data ke pusat, konsep ini memungkinkan pembuatan model yang lebih cerdas, latensi yang lebih rendah, dan konsumsi daya yang lebih sedikit, sekaligus memastikan terjaganya privasi data, dengan model *deep neural network* mampu mempelajari dan mengingat informasi dataset dependensi jarak jauh. Dataset yang digunakan ialah CICIDS 2017, hasil dari train model yang dibuat akan didistribusikan ke CIDS pada masing-masing node.

Kata Kunci: *Deep Learning, Deep Neural Network, Federated Learning, Coordinated Attacks, Collaboration Intrusion Detection System, IDS*