1. PENDAHULUAN

1.1. Latar Belakang

Serangan dunia maya merupakan salah satu tindak kejahatan yang dilakukan oleh para *hacker* dengan tujuan untuk mendapatkan akses secara ilegal atau mengirim kejahatan melalui jaringan komputer yang dituju. Jenis dan teknik penyerangannya pun berbeda-beda, *Coordinated Attacks* (serangan terkoordinasi) adalah penyerangan dilakukan oleh beberapa individu yang bekerja sama secara terencana dan terkoordinasi untuk mencapai target penyerangan dengan peluang keberhasilan lebih besar. *Coordinated Attacks* lebih sulit untuk dideteksi menggunakan *intrusion detection system (IDS)* karena serangan tersebar di beberapa node jaringan. Untuk mengatasi hal tersebut, diperlukannya upaya pendeteksian serangan yang terdistribusi pada setiap node-node jaringan komputer, *collaborative intrusion detection system* dapat digunakan untuk mendeteksi serangan jaringan yang sifatnya terkoordinasi [12].

Collaborative Intrusion Detection System (CIDS) sebuah sistem deteksi intrusion untuk monitoring trafik jaringan dengan cara meletakkan sensor untuk scanning serangan dan pengumpulan data dari setiap node jaringannya, sensor ini akan menangkap dan mendeteksi aktivitas jaringan kemudian sensor mengirimkan data dan mengumpulkannya ke sistem pusat [12]. Sebuah teknologi baru mendeteksi serangan dengan menggunakan algoritma *deep neural network* dan konsep *federated learning* untuk melatih model yang dapat mempelajari suatu pola dan karakteristik dari serangan *coordinated attacks*.

Federated Learning adalah konsep distribusi model, 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 [2][7]. Sebelum adanya konsep *federated learning* pengolahan data dilakukan secara sentral atau terpusat sehingga penggabungan *deep neural network* dengan konsep *federated learning* menjadi salah satu ide solusi dalam permasalahan ini untuk pengolahan data terdistribusi dengan tetap menjaga privasi data disetiap perangkatnya, deep neural network sebuah model yang dirancang untuk dengan beberapa *layers* untuk mengenali fitur yang lebih kompleks pada dataset.

Oleh karena itu, penelitian ini berfokus pada uji coba penggunaan algoritma *deep neural network* dan konsep *federated learning* untuk melatih sebuah model menggunakan dataset CICIDS 2017 dalam mendeteksi *coordinated attacks*, serta menganalisis akurasi dan kecepatan waktu yang dibutuhkan model pada distribusi *centralized learning* dan *federated learning*. Dataset CICIDS2017 yang digunakan hanya beberapa jenis serangan terkooridinasi yaitu *Benign, PortScan, DDoS*, dan *Bot.* Benign adalah aktivitas lalu lintas normal di jaringan, *Portscan* adalah serangan untuk mengintip atau mencari celah *port* yang terbuka pada sistem, kemudian melakukan melakukan serangan melalui *port* yang terbuka [24], *DDoS* adalah serangan *DoS* pada beberapa *host, DDoS* dapat membuat server menjadi down karena mengirimkan trafik palsu secara berlebihan dan bersamaan [17], *Bot* adalah sebuah infeksi komputer yang dilakukan oleh *malware* dan dikendalikan oleh pihak tertentu untuk menyerang komputer target [25]. Konsep *deep neural network* dan *federated learning* akan menjadi salah satu alternatif pengembangan sistem deteksi serangan jaringan.

1.2. Perumusan Masalah

Berdasarkan latar belakang diatas, Berikut merupakan rumusan masalah yang diangkat dalam penelitian.

1. Bagaimana performansi *deep neural network* untuk mendeteksi *coordinated attacks* pada konsep *centralized learning*?
2. Bagaimana performansi *deep nural network* untuk mendeteksi *coordinated attacks* pada konsep *federated learning*?
3. Bagaimana pengaruh jumlah pelatihan setiap klien terhadap akurasi *federated learning*?

1.3. Tujuan

Berdasarkan rumusan masalah diatas, maka tujuan dan manfaat dari penelitian ini adalah sebagai berikut.

1. Membuat simulasi deteksi *coordinated attacks* pada *CIDS* menggunakan algoritma *centralized learning* dan *federated learning.*
2. Mengetahui performansi *deep learning* dalam mendeteksi *coordinated attacks*.
3. Mendapatkat hasil akurasi *federated learning* dari jumlah pelatihan yang berbeda.

1.4. Batasan Masalah

Penelitian ini memiliki batasan masalah sebagai berikut.

1. Mensimulasikan deteksi *coordinated attacks* menggunakan algoritma *centralized learning* dan *federated learning,* algoritma yang digunakan ialah *federated averaging*.
2. Dataset yang digunakan untuk membuat model *deep learning* adalah dataset CICIDS 2017 yang diambil langsung dari website resmi *Canadian Institute for Cybersecurity | University of New Brunswick (UNB)*.
3. Balancing data yang digunakan yaitu metode *ADASYN (Adaptive Synthetic Sampling)*
4. Model *deep learning* yang dilatih hanya untuk mendeteksi serangan jenis *coordinated attacks*, yaitu *PortScan, BOT,* dan *DDoS*.

1.5. Metode Penelitian

1. Studi Literatur
   Penulis melalukan pencarian dan pemahaman dari beberapa research *federated learning* sebelumnya dari paper, jurnal dan sumber terkait lainnya.
2. Eksperimen
   Melakukan uji coba centralized learning dan federated learning lalu membandingkan hasil akurasinya.
3. Analisis Hasil Penelitian
   Hasil dari eksperimen akan dianalisis.
4. Laporan
   Menulis laporan berdasarkan hasil uji coba dan analisis yang dilakukan oleh penulis.