1. Pendahuluan

Latar Belakang

Salah satu ancaman paling signifikan terhadap jaringan dan keamanan adalah serangan DDoS, yang bertujuan membebani sistem dan mengganggu layanan dengan membanjiri lalu lintas dari berbagai perangkat sehingga layanan menjadi tidak dapat diakses. Metode deteksi tradisional sering kali tidak efisien, kurang akurat, dan tidak dapat diskalakan untuk menghadapi serangan yang kompleks dan berskala besar. Tantangan ini muncul karena metode tradisional hanya berfokus pada pemantauan volume lalu lintas dan mendeteksi lonjakan sebagai indikator serangan [1]. Metode deteksi saat ini tidak memadai, sehingga diperlukan pendekatan yang lebih kuat dan efektif untuk menangani serangan DDoS, mengingat karakteristik serangan ini.

Penelitian ini bertujuan mengembangkan pendekatan canggih untuk mendeteksi dan mengklasifikasikan serangan DDoS menggunakan *Multitask Learning* (MTL) dan *Deep Learning* (DL). MTL dapat secara simultan mempelajari adanya ancaman sambil mengklasifikasikan jenis serangan, sehingga meningkatkan efisiensi dan generalisasi [2]. Sementara itu, DL mampu mengenali pola kompleks yang digunakan dalam serangan DDoS dengan secara otomatis menemukan informasi relevan dari data mentah [3]. Kemampuan DL untuk menemukan pola kompleks menjadikannya pilihan ideal untuk deteksi DDoS modern dibandingkan dengan pembelajaran mesin konvensional yang bergantung pada fitur yang telah ditentukan sebelumnya.

Pendekatan deteksi intrusi kolaboratif ini berpotensi meningkatkan keamanan sistem, baik dalam memantau kemungkinan intrusi maupun penyalahgunaan integritas. Dengan menggunakan berbagai dataset dan metode pelatihan yang tepat, keluaran yang optimal dapat dicapai, sehingga kemampuan deteksi yang lebih baik dapat diraih [4][5]. Studi ini mengeksplorasi penggunaan MTL dan DL dalam mendeteksi dan mengklasifikasikan DDoS sebagai alat untuk mengevaluasi teknik-teknik saat ini. Tujuannya adalah menggabungkan keunggulan MTL dan DL untuk membangun model yang lebih efisien, skalabel, dan presisi.

Penelitian ini mengisi celah pada studi sebelumnya oleh Albelwi yang menyoroti perlunya dataset yang lebih kompleks dan algoritma canggih yang mengintegrasikan MTL dan DL [6]. Untuk meningkatkan deteksi dan klasifikasi serangan DDoS, penelitian ini menggunakan dua dataset: NF-CSE-CIC-IDS2018-V2 dan NF-BoT-IoT-V2. Dataset tersebut dipilih karena implementasinya dan fitur-fitur canggihnya yang mampu menangani kompleksitas serangan DDoS modern. Dengan demikian, penelitian ini meningkatkan deteksi dan klasifikasi fitur DDoS, mengatasi kelemahan sebelumnya untuk menghasilkan pendekatan yang lebih kuat dan koheren.