ABSTRAK

*Software Defined Networ*k atau SDN, adalah sebuah pendekatan baru dalam pemrograman jaringan untuk mendesain, membangun, dan mengelola jaringan komputer dengan memisahkan bidang kontrol dari bidang data untuk memusatkan jaringan untuk memusatkan semua pengaturan pada bidang kontrol. SDN dapat secara dinamis memonitor, memodifikasi, dan mengelola perilaku jaringan melalui perangkat lunak antarmuka terbuka.

Pengembangan jaringan sering kali mengalami masalah yang berkaitan dengan keamanan jaringan dan serangan jaringan. Berbeda dengan jaringan konvensional, SDN memiliki berbagai keunggulan, salah satunya adalah SDN dapat mengimplementasikan fungsi kontrol yang terpusat pada *controller*, yang menjadikan controller sebagai jantung dari SDN. Sifat SDN yang tersentralisasi membuatnya menjadi target serangan, salah satunya adalah serangan *Distributed Denial of Service* (DDoS).

Beberapa pendekatan untuk mendeteksi serangan pada SDN telah diusulkan, tetapi hanya sedikit yang mempertimbangkan keamanan *controller*. Oleh karena itu, dibutuhkan sistem keamanan untuk mengatasi masalah serangan yang terjadi pada *controller* SDN. Untuk mengatasi masalah tersebut, dibangun sebuah sistem pendeteksi serangan DDoS dengan menggunakan algoritma *Machine Learning*, yaitu *Random Forest*, yang kinerja algoritmanya dioptimasi dengan menggunakan *Hyperparameter Tuning* untuk mencapai akurasi yang tinggi dalam proses pendeteksian. Dataset InSDN yang terdiri dari total 56 kelas digunakan dalam penelitian ini. Metode ini terbukti efektif dalam mendeteksi serangan DDoS, dengan nilai akurasi sebesar 99,99%. Temuan ini menunjukkan bahwa *Hyperparameter Tuning Random Forest*.

Kata Kunci: Keywords: *Software Defined Network, Distributed Denial of Service, Machine Learning, Random Forest, Hyperparameter Tuning*.