

ABSTRAK

Penggunaan internet sebagai sarana informasi dan komunikasi sangat dibutuhkan. Seiring berkembangnya internet, permasalahan mengenai keamanan komputer menjadi sorotan utama, oleh karena itu sebuah sistem keamanan tambahan diperlukan untuk menanggulangi hal tersebut. *Intrusion Detection System* memiliki andil yang besar dalam permasalahan ini.

Pada penelitian tugas akhir ini menjelaskan bagaimana memprediksi paket yang datang dengan *fuzzy logic*. *Fuzzy logic* digunakan karena *fuzzy logic* dapat menangani sebuah kasus yang mempunyai kebenaran parsial dan informasi yang tidak lengkap. Pada penelitian ini *fuzzy logic* digunakan untuk mengenali kebiasaan atau pola dari paket yang tidak normal, yang nantinya ditindak lanjuti. Dengan menggunakan fungsi keanggotaan dari *fuzzy logic*, penelitian ini dapat menjelaskan perbedaan dari setiap tipe serangan.

Berdasarkan hasil yang diperoleh dengan menggunakan *dataset training* KDDCup'99 10% yang berjumlah 488000 paket, dimana *dataset* terdiri dari paket normal dan paket DOS, akurasi yang didapat sebesar 83%. Menggunakan *dataset training* KDDCup'99 10%, paket selain DOS telah dihilangkan sehingga mempunyai jumlah paket baru sebanyak 387458 paket. *Dataset* ini terdiri dari paket DOS yang mempunyai 6 tipe yaitu *Back*, *Land*, *Neptune*, *Smurf*, *Pod* dan *Teardrop*, akurasi yang didapat sebesar 99% dan presisi sebesar 99%.

Hasil klasifikasi tipe serangan *POD* dan *Neptune* memiliki akurasi sebesar 100%. Perhitungan dilakukan dengan mengambil hasil *cluster* paket *stream* atau *online* secara berkala. Hasil *cluster* *POD* diambil sebanyak 3 kali, *cluster* ke-1 berjumlah 1471 paket, *cluster* ke-2 berjumlah 2907 paket, dan *cluster* ke-3 berjumlah

2777 paket. Hasil *cluster Neptune* diambil sebanyak 3 kali, cluster ke-1 berjumlah 3337 paket, *cluster* ke-2 berjumlah 3266 paket, dan *cluster* ke 3 berjumlah 3282 paket.

Kata kunci : *Intrusion Detection System* , *Fuzzy Logic*.