1. Pendahuluan

Latar Belakang

Perkembangan internet dapat dikatakan pesat semenjak pertama kali digunakan untuk kepentingan militer dan akademik di Amerika Serikat, kini internet sudah mencakup segala aspek kehidupan manusia, mulai dari bidang komunikasi, Pendidikan, hiburan, hingga perbankan. Kompleksitas teknologi yang ada didalamnya pun semakin berkembang dari masa ke masa. Selain itu, ancaman kejahatan siber juga sudah muncul dari tahun 1820 meski saat itu belum ada internet. Kejahatan siber modern ini menyasar kepada data-data pribadi seperti alamat email, data kartu kredit, alamat rumah, detil identitas d.l.l.

Salah satu jenis serangan internet adalah DoS, serangan DoS pertama kali yang terdokumentasikan adalah pada 7 Februari 2000 yang menimpa beberapa situ e-commerce di Amerika Serikat seperti Amazon, e-Bay. Sejak saat itu serangan DoS terus berkembang dan berevolusi menjadi lebih efektif dan berbahaya. Contoh serangan DoS lain yang menarik perhatian dunia adalah serangan DoS di Estonia pada tahun 2007, dimana serangan DoS di negara itu dapat melumpuhkan jaringan internet seluruh negara [4].

Dari kejadian-kejadian diatas, dapat dilihat bahwa DoS memiliki peran dan tingkat berbahaya yang tinggi, hal ini mendorong peneliti-peneliti di dunia untuk mempelajari DoS dan melakukan deteksi lebih awal terhadap serangan DoS. Deteksi serangan dengan DoS dapat diklasifikasikan menjadi dua kategori, misuse detection dan anomaly detection [3]. Deteksi DoS yang efektif serta dapat memberikan jaminan kemanan adalah system deteksi yang dapat berjalan secara real time [4].Kebutuhan lainnya dalam upaya ini adalah klasifikasi DoS menggunakan algoritma *Machine Learning* yang efektif dan efisien sehingga memiliki akurasi yang tinggi dan waktu deteksi serta *training* data yang lebih cepat. Selain itu Sistem deteksi DoS komersial memiliki tingkat alarm palsu yang tinggi, menghasilkan ratusan alarm palsu per hari karena seringkali sulit untuk memilih secara manual kondisi identifikasi untuk sejumlah besar serangan dan varian mereka[9], sehingga dibutuhkan *Artificial Intelligence* guna membantu menyelesaikan masalah ini.

Shiaeles, Katos, Karakos a, Papadopoulos[4] mengembangkan Real Time DoS Detection dengan menggunakan fuzzy estimator dan dapat menghasilkan akurasi 80%. Sedangkan Hoque, Kashyap, Bhattacharyya[6] melakukan Real Time DoS Detection dengan metode FPGA (Field Programmable Gate Arrays) mampu mendeteksi dengan tingkat akurasi mencapai 100% dengan menggunakan NaHiDVERC (NaHiD for DoS detection using Variation, Entropy of Source IPs and Packet Rate) yang diterapkan menggunakan FPGA, namun DoS oleh NaHiDVERC masih dianggap sebagai masalah kelas dua, sehingga masih harus ada perbaikan. Namun, ketiga metode diatas masih dapat dikembangkan untuk mencapai akurasi deteksi yang lebih baik lagi dengan metode yang berbeda digabungkan dengan arsitektur IDS yang tepat.

Permasalahan lainnya adalah teknik klasifikasi yang tidak memiliki waktu *training* yang singkat menyebabkan waktu deteksi juga menjadi lamban, maka dari itu akan dilakukan percobaan dengan tujuan untuk mencari waktu *training* yang lebih cepat pada klasifikasi DoS serta tetap menghasilkan akurasi yang baik.

Topik dan Batasannya

1. Klasifikasi dataset untuk deteksi DoS.
2. Menghitung waktu *training*.
3. Menggunakan algoritma *Artificial Neural-Network*.
4. Mengetes model klasifikasi dataset NSL KDD terhadap datalog.

Tujuan

- Mengukur akurasi klasifikasi DoS menggunakan *artificial Neural-Network*.
- Mengetes model NSL KDD terhadap datalog.