1. Pendahuluan

1.1 Latar belakang

IDS berbasis deteksi anomali memiliki keuntungan dalam mendeteksi serangan yang sebelumnya belum pernah diketahui (*zero day attack*). IDS akan mengenali trafik jaringan yang "normal" (baca: terbebas dari serangan), untuk kemudian dibentuk model yang dibangun berdasarkan database trafik yang "normal" tersebut. Kemudian IDS akan membangkitkan alarm bila ternyata ada trafik "abnormal", yaitu dasta uji yang memiliki deviasi terhadap model yang secara signifikan melebihi threshold. Namun pada IDS berbasis anomali ini terdapat masalah, yaitu memiliki false negative yang relatif tinggi. Oleh karena itu, untuk memperoleh hasil deteksi yang akurat, dibutuhkan algoritma yang tepat dalam mengklasifikasi kenormalan data trafik.

Self-Organizing Maps (SOM) dapat digunakan untuk mempelajari pola trafik normal dari data historis yang ada. SOM memiliki kemampuan klasifikasi (similaritas intra-cluster dan dissimilaritas inter-cluster) yang tinggi [1][10], mampu memvisualisasi data berdimensi tinggi ke dalam data berdimensi kecil (umumnya dua dimensi) dan juga memiliki performansi real-time [7]. Algoritma SOM dapat juga digunakan untuk proses deteksi anomali, yaitu dengan cara membandingkan quantization error antara input vector terhadap hasil clustering SOM. Meskipun demikian, algoritma SOM mempunyai beberapa kelemahan, antara lain komputasi yang relatif tinggi, membutuhkan *learning time* yang cukup lama dan pencarian Best Matching Unit (BMU) yang relatif lama. Hal ini mempertimbangkan banyaknya kasus penyerangan terhadap banyak *victim* secara cepat,salah satu contohnya adalah kasus worm code red. Metode deteksi dengan SOM juga memiliki kekurangan, karena hasil quantization error-nya dapat dipengaruhi oleh urutan byte payload.

Untuk mengatasi masalah dan memangkas komputasi algoritma SOM di atas dibutuhkan adanya improvisasi atau pendekatan lain yang mampu meningkatkan performansi tanpa mempengaruhi akurasi algoritma SOM. Algoritma Fast Winner Search merupakan salah satu algoritma yang mampu meningkatkan performansi algoritma SOM melalui pencarian BMU dengan cara menghitung inner product terbesar dari normalisasi input vector terhadap bobot unit pada jaringan yang dibangun algoritma SOM. Sementara itu, Algoritma N-Gram dapat mengatasi masalah deteksi dengan cara menghitung frekuensi kemunculan byte dalam membangun model normal, dan membandingkannya dengan input vector.

1.2Perumusan masalah

Masalah yang dikaji dan diselesaikan dalam tugas akhir ini adalah Analisis dan Implementasi Algoritma Fast Winner Search dan N-Gram pada Network Intrusion Detection System.

Masalah-masalah khusus yang berkaitan dengan masalah ini adalah :

1. Bagaimana mengimplementasikan algoritma Fast Winner Search dan N-Gram pada Intrusion Detection System?
2. Bagaimana mengukur akurasi Algoritma Fast Winner Search dan N-Gram yang dibangun pada Intrusion Detection System?

1.3 Batasan masalah

Untuk menghindari pembahasan yang panjang tetapi dangkal, maka pada tugas akhir ini pembahasan hanya dibatasi pada :

1. Menggunakan data trafik offline yang diperoleh dari dataset DARPA IDS 1999 [3].
2. Asumsi dataset yang bersifat normal (terbebas dari serangan), jauh lebih banyak daripada dataset yang abnormal (berisi serangan).
3. Hanya menganalisis paket inbound TCP dengan alamat tujuan 172.016.0.0/16 dan port tujuan 1-1024.
4. Penggunaan pendekatan Fast Winner Search dilakukan pada pencarian Best Matching Unit (BMU).

1.4 Tujuan

Berdasarkan penjelasan diatas, penulis terdorong untuk melakukan hal-hal yang dirumuskan dalam tujuan pembahasan “Analisis dan Implementasi Algoritma Fast Winner Search dan N-Gram pada Network Intrusion Detection System”.

Secara lengkap, pembahasan dalam tugas akhir ini dilakukan untuk :

1. Menerapkan algoritma Fast Winner Search dan N-Gram pada Intrusion Detection System.
2. Mengukur akurasi algoritma Fast Winner Search dan N-Gram dalam mendeteksi intrusi

Hipotesis :

Algoritma Fast Winner Search pada Self-Organizing Maps dan N-Gram mampu mendeteksi intrusi dengan akurasi yang baik dan waktu yang singkat

1.5 Metodologi penyelesaian masalah

1. Studi literatur
   Merupakan tahapan dalam mempelajari konsep dan teori pendukung untuk memecahkan permasalahan.Dalam tugas akhir ini, studi literatur meliputi pembelajaran Neural network, datamining dan konsep lainnya yang menunjang pembuatan tugas akhir ini.
2. Pengumpulan data
   Pada tahap ini, pengumpulan data hanya melakukan pengunduhan dataset DARPA IDS 1999 pada alamat [3].
3. Analisis dan perancangan sistem
   Pada tahap ini, dianalisis kebutuhan sistem dan dibentuk sebuah *blueprint* yang akan dijadikan sebagai acuan dalam tahap berikutnya, yaitu bagaimana melakukan implementasi sistem dan pengujian.
4. Implementasi dan pembangunan sistem
   Tahap ini merupakan realisasi dari *blueprint* yang telah dbentuk dengan cara *coding* menggunakan bahasa pemrograman MATLAB dalam pengerjaannya. Pertama-tama data trafik jaringan diklasifikasi dengan menggunakan algoritma gabungan Self Organizing Maps dengan Fast Winner Search. Setelah ditemukan *winning neuron*-nya, sistem akan membentuk pola trafik dengan menghitung mean dan standar deviasi berdasarkan winning neuron, port tujuan dan alamat host tujuan kemudian menghitung similaritas antara pola trafik yang telah dilatih dengan data trafik. Jika jarak antar keduanya melebihi treshold secara signifikan, maka payload data trafik tersebut merupakan sebuah *attack.*
5. Pengujian dan analisa hasil
   Tahap ini melakukan pengukuran terhadap hasil akurasi deteksi intrusi yang telah dibangun.
6. Pembuatan Laporan
   Pada tahap ini diambil kesimpulan terhadap setiap informasi yang penting untuk dapat disajikan pada laporan ilmiah.

1.6 Sistematika penulisan

Tugas akhir ini disusun dengan sistematika penulisan sebagai berikut:

1. Pendahuluan
   Bab ini berisi uraian tugas akhir secara umum, meliputi latar belakang masalah, perumusan masalah, batasan masalah, tujuan, metodologi penyelesaian masalah, dan sistematika penulisan laporan.

2. Landasan Teori
   Bab ini menguraikan teori intrusion detection system (IDS), algoritma Self-organizing Maps, metode Fast Winner Search, metode n-gram dan perhitungan jarak mahalanobis.
3. Analisis Perancangan dan Implementasi
   Bab ini membahas mengenai perancangan sistem untuk melatih model yang menggabungkan algoritma Self-organizing Maps dan Fast Winner Search. Hasil dari perancangan kemudian digunakan dalam proses implementasi sistem.
4. Pengujian dan Analisis Hasil Percobaan
   Bab ini berisi pengujian hasil implementasi yang telah dilakukan pada bab sebelumnya. Pengujian dilakukan dengan mengukur Akurasi, True Positive Rate,True Negative Rate, False Positive Rate dan False Negative Rate. Setelah pengujian selesai, dilakukan analisis terhadap hasil pengujian yang ada.
5. Kesimpulan dan Saran
   Bab ini berisi kesimpulan dari penulisan tugas akhir dan saran – saran untuk pengembangan lebih lanjut.