BAB I

PENDAHULUAN

1.1. Latar Belakang

Supervisory Control And Data Acquisition (SCADA) adalah *Industry Control System* (ICS) otomatis yang digunakan untuk memonitoring dan mengendalikan proses di sektor industri dan sektor infrastruktur *Critical* nasional. Seperti pembangkit dan distribusi energi dan jaringan tenaga listrik. Secara historis system SCADA dirancang dengan jaringan *private network,* namun karena penyebaran perangkat SCADA secara geografis, sekarang komunikasi SCADA menggunakan internet.

Salah satu protocol komunikasi SCADA adalah IEC 60870-5-104 atau dikenal juga sebagai IEC104 yang dimana digunakan untuk mengirim pesan telekontrol dasar antar perangkat berdasarkan standar TCP/IP, yang memungkinkan transmisi data secara simultan antara beberapa perangkat dan layanan. Protocol IEC104 memiliki kerentanan pada keamanan *application layer* dan *data link layer.* Kerentanan pada *application layer* menyebabkan protocol ini dapat diserang dengan *spoofing.* Pada *data link layer* menyebabkan protocol ini dapat di serang menggunakan *snipping, modification data* dan *replay attack.*

Terdapat banyak serangan *cyber* yang bisa terjadi di system SCADA, salah satu nya serangan *Man In The Middle* (MITM) yang mempunyai risiko sangat tinggi bagi jaringan SCADA. Serangan MITM adalah sebuah proses serangan dimana *hacker* menyelinap di tengah-tengah sebuah koneksi untuk mendapatkan informasi tanpa diketahui, memodifikasi, memotong koneksi dan bahkan dapat mencuri data yang sangat penting.

Ada pendekatan yang dapat digunakan untuk mencegah hal tersebut yaitu menggunakan *Intrusion Detection System* (IDS). IDS merupakan system yang sangat penting dalam keamanan jaringan, dimana IDS berfungsi untuk mendeteksi kemungkinan adanya serangan oleh *attacker.*

Beberapa metode digunakan untuk IDS, yaitu *signature based* dan *anomaly based.* seperti pada penelitian (Chambali : 2020) *"*Klasifikasi Paket

Jaringan Berbasis Analisis Statistik dan *Neural Network"* menjelaskan bahwa kekurangan dari signature based yaitu meningkatnya volume alert yang bersifat false-positive yang mengakibatkan rendahnya efisiensi. maka dirancang anomaly based berbasis *machine learning Neural Network* untuk mengklasifikasi serangan, dan mendapatkan akurasi sebesar 92,99%.

Salah satu penggunaan IDS pada jaringan SCADA termasuk konsep yang relatif baru. Pada penelitian (Hodo : 2017) "Anomali detection for simulated IEC-60870-5-104 traffic," membahas tentang sistem deteksi anomaly based berdasarkan protocol IEC104, menggunakan tiga model serangan yaitu, *Arp Spoofing, DoS* dan *Command Injection*. Model deteksi diracangan dengan algoritma *Supervised Learning*, dari hasil pengujian didapat bahwa algoritma *Rule Learners* memiliki akurasi terbaik yaitu 91,69%.

Salah satu penelitian (Ahmad : 2018) "Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection" untuk membandingkan algoritma Supervised Learning yaitu *Support Vector Machine*, *Random Forest*, dan *Extreme Machine Learning* sebagai *Intrusion Detection System* pada jaringan NSL-KDD, Hasilnya *extreme learning machine* unggul di sampel data lengkap dan *support vector machine* menunjukkan hasil yang lebih baik di setengah dan seperempat sampel data.

Berdasarkan penjelasan di atas, karena rentannya jaringan SCADA terhadap serangan MITM sehingga membutuhkan IDS untuk mencegahnya. Berdasarkan hal tersebut, maka penelitian Laporan akhir ini akan mengusulkan algoritma *intrusion detection system anomaly based* menggunakan pendekatan *supervised learning* dengan judul **Klasifikasi Serangan *Man In The Middle* (MITM) Menggunakan *Support Vector Machine* Pada Jaringan *Supervisory Control and Data Acquisition* (SCADA)**.

1.2. Rumusan Masalah

Adapun rumusan masalah dalam penelitian Tugas Akhir ini adalah sebagai berikut:

1. Bagaimana cara mengekstrak dataset, kemudian mengklasifikasikan serangan *Man In The Middle.*
2. Bagaimana metode *Support Vector Machine* dapat mengenali serangan *Man in The Middle* pada jaringan *Supervisory Control And Data Acquisition* pada dataset.
3. Bagaimana memvisualisasikan pola serangan *Man In The Middle* kedalam bentuk grafis

1.3. Batasan Masalah

Berikut adalah batasan masalah dalam penelitian Tugas Akhir ini:

1. Pengujian dilakukan pada data csv yang didapatkan dari jaringan *Supervisory Control And Data Acquisition* protokol IEC ASDU 60870-5-104.
2. Mengklasifikasi serangan *Man In The Middle* pada jaringan *Supervisory Control And Data Acquisition* menggunakan *Support Vector Machine.*
3. Serangan yang dideteksi hanya serangan *Man in The Middle* pada dataset.
4. Menggunakan *dataset* dalam bentuk yang ter*capture traffic* normal dan serangan *Man in The Middle.*
5. Jumlah data pada dataset yang digunakan sebanyak 35815 sesuai jumlah data pada protokol IEC ASDU 60870-5-104.
6. Dataset akan dibagi menjadi 2 yaitu data uji 20% dan data training 80%
7. Klasifikasi serangan *Man In The Middle* tidak diujikan pada lalu lintas jaringan real-time.
8. pengujian secara *offline.*
9. tidak membahas cara pencegahan serangan *Man in The Middle.*

1.4. Tujuan

Adapun tujuan dari penelitian Tugas Akhir ini adalah sebagai berikut :

1. Membedakan antara trafik normal dan trafik serangan pada jaringan *Supervisory Control And Data Acquisition* sehingga dapat mendeteksi serangan *Man In The Middle.*
2. Menerapkan algoritma *Support Vector Machine* untuk deteksi trafik serangan *Man In The Middle* pada jaringan *Supervisory Control And Data Acquisition*
3. Memvisualisasi data normal dan serangan *Man In The Middle* dalam bentuk grafik.
4. Menganalisa Keakurasian Metode *Support Vector Machine* untuk mengklasifikasi serangan *Man In The Middle* pada jaringan *Supervisory Control And Data Acquisition.*

1.5. Manfaat

Adapun manfaat dari penelitian Tugas Akhir ini adalah sebagai berikut :

1. Dapat membedakan trafik serangan dan trafik normal pada jaringan *Supervisory Control And Data Acquisition*
2. Dapat mendeteksi serangan *Man in The Middle* pada jaringan *Supervisory Control And Data Acquisition*
3. Dapat mengetahui tingkat akurasi metode *Support Vector Machine* dalam klasifikasi serangan *Man in The Middle* pada jaringan *Supervisory Control And Data Acquisition*.