BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Penggunaan jaringan internet kini semakin meluas. Tidak hanya digunakan untuk individu tetapi juga sesuai untuk organisasi, institusi atau perusahaan untuk memfasilitasi pertukaran data dan informasi secara bersama-sama. Terkadang data atau informasi tersebut bersifat pribadi dan begitu penting sehingga diperlukan keamanan agar tidak jatuh ke pihak yang tidak bertanggung jawab. Keamanan jaringan harus diperhatikan dalam mengembangkan jaringan komputer untuk mencegah serangan dari pihak yang jahat.

Konektivitas yang semakin meluas dalam sistem informasi saat ini menimbulkan tantangan baru bagi keamanan. Mekanisme keamanan konvensional telah berhasil mencapai tujuan kerahasiaan, integritas, orisinalitas, dan ketersediaan yang terdefinisi dengan baik. Namun, dengan meningkatnya kompleksitas sistem dan jangkauan serangan, memberikan keamanan melalui metode tradisional semakin sulit dicapai (Anwar dkk, 2020).

Menurut informasi dari Pusat Keamanan Operasi Siber Badan Siber dan Sandi Nasional Indonesia, selama tahun 2019, sistem titik pantau elang mendeteksi sekitar 290,3 juta serangan siber (intrusi) ke dalam jaringan internet Indonesia. Yang terbesar adalah serangan uji kebocoran data, diikuti dengan serangan menggunakan metode *malware*. Dibandingkan dengan banyaknya serangan siber, jumlah pengaduan masyarakat tentang insiden yang terjadi relatif sedikit, serangan siber melonjak tajam pada September, Oktober, dan menurun tajam pada November. Pada November dan Desember, angka ini masih jauh lebih tinggi dibandingkan 6 bulan pertama tahun 2019-

an. Salah satu penyebab tingginya tingkat serangan siber adalah karena acara tersebut pasti akan melibatkan banyak orang, misalnya pada bulan Oktober bertepatan dengan pelantikan Presiden dan Wakil Presiden Indonesia periode baru 2019-2024.

Penelitian Keamanan Jaringan menjadi pusat perhatian mengingat kerentanan ekosistem komputasi dengan sistem jaringan yang semakin beralih ke tangan peretas. Pada kanvas keamanan jaringan, sistem deteksi intrusi adalah alat penting yang digunakan untuk mendeteksi serangan dunia maya secara tepat waktu. *Machine Learning* sering digunakan untuk mendeteksi intrusi karena pemahaman mereka tentang sistem deteksi intrusi dalam meminimalkan ancaman keamanan. Namun, beberapa pengklasifikasi tunggal memiliki keterbatasan dan menimbulkan tantangan bagi pengembangan *Intrusion Detection System* yang efektif (Bamhdi dkk, 2021).

Identifikasi serangan dalam jaringan komputer dibagi menjadi dua kategori, yaitu deteksi intrusi dan deteksi anomali dari segi informasi yang digunakan dalam tahap pembelajaran. Deteksi intrusi menggunakan lalu lintas rutin dan lalu lintas serangan. Metode deteksi abnormal mencoba untuk memodelkan perilaku normal sistem, dan setiap kejadian yang melanggar model ini dianggap sebagai perilaku yang mencurigakan (Majidpour & Hasanzadeh,2020).

Keamanan komputer didefinisikan sebagai teknik dan prosedur administrativ yang diterapkan pada sistem komputer untuk memastikan ketersediaan, efektivitas, dan kerahasiaan transfer informasi dalam sistem komputer dan memastikan akses. Keamanan komputer dapat diklasifikasikan menjadi tiga bidang yaitu pencegahan, deteksi dan reaksi. Area kedua dicakup oleh sistem deteksi intrusi atau biasa disebut *Intrusion Detection System* (IDS), didefinisikan sebagai identifikasi dan respons dari setiap perilaku jahat yang menargetkan sumber daya komputer dan jaringan. Ini dapat diklasifikasikan menjadi dua jenis utama: basis tanda tangan dan basis penyalahgunaan. Basis tanda tangan bergantung pada tanda tangan penyerang, sedangkan basis penyalahgunaan bertindak untuk menemukan perilaku abnormal dari pengguna (Thabit, H. & Yaser, A. J., 2017).

IDS didefinisikan sebagai pekerjaan yang menggunakan teknik dan mekanisme khusus untuk mendeteksi gangguan. Intrusi didefinisikan sebagai upaya untuk mengkompromikan keamanan, efektivitas, atau mekanisme keamanan yang tumpang

tindih dalam suatu sistem atau jaringan. IDS memonitor dan menganalisa kejadian-kejadian dalam sebuah komputer atau sistem jaringan untuk mendeteksi tanda-tanda penyusupan, dimana sistem deteksi penyusupan adalah komponen yang dapat diprogram atau fisik yang bekerja secara otomatis pada pemantauan seperti yang disebutkan di atas untuk mengidentifikasi masalah keamanan. Penyerang yang mengganggu sistem dengan masuk sebagai pengguna jaringan yang sah untuk mendapatkan hak istimewa tambahan dari pengguna biasa yang tidak sah dan pengguna sah yang menyalahgunakan hak yang diberikan kepada mereka. Namun IDS mendeteksi serangan atau perilaku abnormal yang terjadi di dalam jaringan dan segera mengeluarkan alarm yang mengetahui orang yang bertanggung jawab atas keamanan di jaringan saat serangan terjadi dan memintanya untuk mengambil tindakan yang diperlukan (Jasim, 2018).

Menguji sistem pendeteksian serangan atau penyusupan menggunakan metode seleksi fitur dengan menggunakan dataset UNSW-NB-15. Hasil penelitian menunjukkan bahawa metode *XGBoost-based feature selection* meningkatkan ketepatan pengujian dari 88.13% hingga 90.85% untuk skema binary *classification (*Kasongo & Sun, 2020).

Membandingkan Teknik *Machine Learning*, yaitu, SVM, *Random Forest*, dan *Extreme Learning Machine* (ELM) yang diterapkan pada Dataset NSL-KDD. Ketiga teknik yang disebutkan diuji kemampuannya dalam klasifikasi. Dataset NSL-KDD digunakan karena dianggap sebagai penanda aras dalam penilaian mekanisme pendeteksian pencerobohan. Hasilnya menunjukkan bahawa ELM mengatasi metode lainnya (Ahmad dkk, 2018).

Pengusulkan penggunaan algoritma metode seleksi *hybrid* dengan *Guided Regularized Random Forest-Feature Weighting* SVM (GRRF-FWSVM) + Cat Boost dan diterapkan pada dataset KDD 99 Cup. Hasil penelitian menunjukkan bahwa metode pemilihan fitur hybrid yang diusulkan dengan klasifikasi GRRF-FWSVM + *CatBoost* sebesar 98,55% pada set pengujian dibandingkan dengan dua model benchmark lainnya. Model yang diusulkan telah mencapai tingkat kinerjanya dengan tingkat akurasi yang tinggi (Kavitha & Elango, 2020).

Pengusulkan penggunaan algoritma *Convolutional Neural-based learning Classifier System* (CN-LCS) yang merupakan model gabungan antara *Learning Classifier System* (LCS) konvensional dengan *Convolutional Neural Network* (CNN)

yang diterapkan pada *synthetic query dataset*. Kombinasi LCS gaya Pittsburgh yang diubah sesuai untuk pengoptimuman peraturan *feature selection* dan penggunaan CNN satu dimensi untuk pemodelan dan klasifikasi sebagai ganti peraturan tradisional mengatasi pengeluar pembelajaran mesin yang lain (Bu & Cho, 2020).

Penggunakan algoritma *Convolutional Neural Networks* (CNN) dengan membandingkannya dengan *Recurrent Neural Network* (RNN) pada dataset NSL-KDD. Sejumlah besar *Data Mining* (DM), *Machine Learning* (ML), dan teknik kecerdasan buatan digunakan dalam pengembangan IDS, banyak dari penelitian sebelumnya di bidang ini telah berfokus pada penggunaan algoritma klasifikasi dan teknologi agregasi untuk meningkatkan operasi deteksi intrusi. Penelitian ini digunakan untuk meningkatkan kinerja IDS (akurasi tinggi, tingkat deteksi, dan mengurangi tingkat alarm palsu) (Wu dkk, 2018).

Peneliti mencadangkan model bersatu yang menggabungkan *Multiscale Convolutional Neural Network dengan Long Short-Term Memory* (MSCNN-LSTM). Model ini pertama kali menggunakan *Multiscale Convolutional Neural Network* (MSCNN) untuk menganalisis ciri spasial dataset, dan kemudian menggunakan Jaringan *Long Short-Term Memory* (LSTM) untuk memproses ciri temporal. Menggunakan Set Data UNSW-NB15. Hasil eksperimen menunjukkan bahawa hasil MSCNN-LSTM l tersebut dapat meningkatkan ketepatan dengan berkesan berbanding dengan metode lain yang ada dan secara efektif mengurangkan FAR kerana secara automatik mempelajari ciri-ciri spasial-temporal, yang meningkatkan prestasi keseluruhan IDS (Zhang dkk, 2020).

Peneliti membangun DL-IDS (*deep learning based intrusion detection system*), yang menggunakan rangkaian *hibrid Convolutional Neural Network* (CNN) dan *Long Short-Term Memory Network* (LSTM). Menggunakan Set Data CICIDS2017. Hasilnya menunjukkan bahawa DL-IDS masing-masing mencapai 98.67% dan93.32% dalam keseluruhan ketepatan dan skor F1, yang menunjukkan prestasi yang lebih baik daripada semua model pembelajaran mesin. Juga, dibandingkan dengan model CNN-only dan model LSTM sahaja, DL-IDS mencapai lebih dari 99.50% dalam ketepatan semua jenis serangan dan mencapai prestasi terbaik di antara ketiga-tiga model ini (Sun dkk, 2020).

Peneliti mengusulkan model pembelajaran mendalam yang dibangun berdasarkan lapisan jaringan saraf convolutional (CNN) dan menggunakan lapisan Memori Jangka Pendek (LSTM) yang disebut CNN-LSTM untuk mengklasifikasikan setiap jaringan lalu lintas. Menggunakan kumpulan data NSL-KDD. NLS-KDD memiliki dua set tes yaitu KDDTest+ dan KDDTest-. Banyak penelitian hanya berfokus pada KDDTest+ karena lebih mudah untuk diklasifikasikan daripada KDDTest-. Namun, metode yang diusulkan dapat menggantikan metode lain yang tersedia di KDDTest+ atau KDDTest- (Hsu dkk, 2021).

Peneliti mengusulkan model deteksi intrusi jaringan multiklasifikasi berdasarkan jaringan saraf *convolutional*, dan algoritma yang dioptimalkan. Penelitian menggunakan Dataset KDD-CUP 99 dan NSL-KDD. Dalam penelitian ini, peneliti membandingkan hasil eksperimen dengan model *deep learning* DNN, LSTM-RNN, GRU-RNN, DBN, KNN, ICNN, dan sebagainya. Hasil eksperimen menunjukkan bahwa model deteksi intrusi jaringan yang diusulkan meningkatkan akurasi dan retraksi berkurangn kadar positif palsu, dan memperoleh hasil pendeteksian yang lebih baik untuk mendeteksi serangan yang tidak diketahui (Liu & Zhang, 2020).

Penelitian mengusulkan sistem deteksi intrusi baru yang disebut TR-IDS, yang memanfaatkan fitur statistik dan fitur muatan dengan mengimplementasikan penyematan Word dan jaringan saraf konvolusi teks (Text-CNN) untuk mengekstrak informasi dari muatan secara efektif. Menggunakan kumpulan data ISCX2012. Teknik penyisipan kata mempertahankan hubungan semantik antara setiap byte dan mengurangi dimensi fitur, dan kemudian Text-CNN digunakan untuk mengekstrak fitur dari setiap beban. Eksperimen ekstensif menunjukkan kinerja unggul dari metode yang diusulkan (Min dkk, 2018).

Untuk membangun sebuah IDS, diperlukan kinerja sistem yang mumpuni agar dapat berjalan normal. Seluruh proses pendeteksian harus dapat dilakukan dalam jumlah besar sekaligus dengan menerapkan arus. Bahasa pemrograman Go dapat menangani kasus kasus seperti yang ditemui. Salah satu pilar inti Go adalah fitur pemrograman kurikulernya, termasuk penguncian memori bersama untuk sinkronisasi thread, dan penggunaan saluran penerusan pesan eksplisit (Gabet & Yoshida, 2020).

Berdasarkan penelitian ini dalam Langkah memberikan perlindungan pada server terhadap intrusi yang ada digunakan IDS secara *real time* menggunakan seleksi fitur dan *firebase cloud mesaaaging.*

1.2 Perumusan Masalah

Setiap server tentunya memiliki konfigurasi yang berbeda, diperlukan solusi agar IDS dapat berjalan di berbagai server dengan konfigurasi yang fleksibel dan minimal. Mengingat keterbatasan penelitian sebelumnya, pertanyaan berikut akan dibahas dalam penelitian ini:

1. Bagaimana menerapkan algoritma *feature selection* sehingga dapat membantu proses pemilihan fitur yang tidak berlebihan dan relevan dengan kebutuhan untuk menangani serangan server?
2. Bagaimana mencapai tingkat deteksi serangan pada server yang memuaskan di tengah lalu lintas jaringan yang sangat padat yang sering diklasifikasikan sebagai anomali deteksi oleh IDS.

Bagaimana membuat sebuah aplikasi untuk mendeteksi serangan atau penyusupan terhadap sebuah web server dan menampilkan alert hasil deteksi kepada administrator dalam bentuk *firebase messaging*. Maka diangkat penelitian ini dengan judul Sistem diteksi intrusi pada server secara realtime menggunakan seleksi fitur dan firebase cloud messaging.

1.3 Batasan Masalah

Batasan masalah pada penelitian ini adalah membuat sebuah sisten peringatan untuk mendeteksi aktivitas yang dianggap mencurigakan pada server berdasarkan rule yang telah di tentukan melalui hasil pengolahan *machine learning* dari *dataset* yang telah ditentukan dengan menggunakan algoritma *feature selction*. Peringatan aktivitas

yang mencurigakan akan diteruskan oleh server ke aplikasi monitoring yang dipegang oleh admin server dengan menggunakan teknologi *firebase cloud massaging* sebagai pengirim pesan peringatan secara *realtime*.

1.4 Tujuan Penelitian

Tujuan utama dari penelitian ini adalah untuk mengembangkan sistem deteksi intrusi server yang efisien menggunakan teknologi pembelajaran mesin. Untuk mencapai tujuan ini, sub-target berikut telah diidentifikasi:

1. Identifikasi karakteristik dasar trafik server mulai dari menggunakan fase *pre-processing* hingga fase *post-processing*.
2. Menggunakan algoritma *feature selection* dalam proses pemilihan fitur yang tidak berlebihan dan relevan dengan kebutuhan untuk menentukan jenis serangan pada server.

Kontribusi dari penelitian ini adalah untuk meningkatkan pengetahuan aplikasi machine learning ke IDS dan untuk menghasilkan IDS yang efisien sehingga produk yang dihasilkan ini nantinya diharapkan dapat digunakan dan dimanfaatkan oleh masyarakat luar dengan mudah untuk mengamankan dan mendeteksi gangguan pada server mereka.

1.5 Manfaat Penelitian

Penelitian ini bertujuan untuk dapat memberikan manfaat yang dapat berguna bagi yang membutuhkan penelitian sejenis, adapun manfaat yang dapat dirasakan dari penelitian ini adalah sebagai berikut:

1. Dapat memahami cara kerja dari beberapa IDS.

2. Mengetahui jalur mana saja yang sering digunakan penyusup agar nantinya dapat dilakukan pemblokiran sehingga tidak dimanfaatkan kembali.

1.6 Sistematika Penulisan

Sistematika penulisan disesauaikan dengan format yang diatur dalam tata penulisan Tesis Program Studi Strata 2 Megister Ilmu Komputer, Berdasarkan hal itu, peneliti mengklasifikasikan penelitian ini kedalam enam bab, di mana antara bab satu dengan bab yang lain saling berhubungan. sebagai berikut:

Bab I Pendahuluan

Pada BAB I ini berisikan latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan Sistematika penulisan.

Bab II Landasan Teori

Pada BAB II ini berisikan tentang landasan teori yang bertujuan untuk menjelaskan penerapan, prosudur, pengertian dan berbagai hal yang berhubungan dengan judul yang diangkat.

Bab III Metodologi

Pada BAB III ini berisikan bahasan dan menjelaskan tetang kerang kerja ataupun tahapan-tahapan yang harus dilalui dalam penelitian ini.

Bab IV Analisa

Pada BAB IV ini berisi tentang pembahasan prosudur didalam penggunaan dan pemanfaatan *feature selection,* pembuatan aplikasi IDS, aplikasi peringatan dengan menggunakan *Firebase Cloud Messaging*.

Bab V Implementasi dan Pengujian

Pada BAB V ini akan membahas bagaimana implementasi *feature selection* dalam menyeleksi serangan, bagaimana melakukan instalasi IDS ke dalam server dan bagaimana cara IDS memberikan notifikasi kepada Network Administrator.

Bab VI Simpulan Dan Saran

Pada BAB VI akan memberikan beberapa kesimpulan dari hasil penelitian dan saran.