OPTIMIZATION OF INTRUSION DETECTION SYSTEM WITH MACHINE LEARNING FOR DETECTING DISTRIBUTED ATTACKS ON SERVER

OPTIMALISASI SISTEM DETEKSI INTRUSI MENGGUNAKAN MACHINE LEARNING UNTUK DETEKSI SERANGAN TERDISTRIBUSI PADA SERVER

Teddy Yuliswar[1], Ikhwana Elfitri[2], Onno W Purbo[3]
[1,2] Departemen Teknik Elektro, Fakultas Teknik, Universitas Andalas, Kota Padang, Sumatera Barat
[3] Institut Teknologi Tangerang Selatan (ITTS), Kota Tangerang Selatan, Banten, Indonesia
Email: 2120952005_Teddy@student.unand.ac.id, ikhwana@eng.unand.ac.id[2], onno@indo.net.id[3]

Abstract *- This study develops an intrusion detection system optimized with machine learning techniques for efficient and effective detection of Distributed Denial-of-Service (DDoS) attacks. Using the Decision Tree algorithm, the system is designed to maximise accuracy in the identification and classification of DDoS attacks. The CIC-DDoS2019 dataset, which consists of various comprehensive simulated attack scenarios, is used as the basis for training and validation, providing the model with robust capabilities in recognizing DDoS attacks with high accuracy. This IDS successfully achieved a 100% detection rate, which is a significant result in the network security environment. The system is integrated into the existing network infrastructure, monitoring data flows in real-time and performing predictive analysis to detect early indications of attacks. Each attack detection immediately triggers a notification sent via a Telegram bot, ensuring that the security team can react quickly to isolate and address the attack. These notifications include details such as the source, type of attack, detection time, and involved protocol information, enabling more informed and strategic response actions. The use of Telegram bots for real-time communication not only enhances the speed of response to threats but also supports system scalability by facilitating adjustments and integration across various operational scenarios. The system's quick detection and response is a big step forward for machine learning-based intrusion detection systems (IDS). It provides opportunities for further research and practical applications that can adapt to various digital security scenarios.*

Keywords *– Intrusion Detection System, Machine Learning, DDoS, Decision Tree, CIC-DDoS2019 Dataset*

Abstrak - Studi ini mengembangkan sistem deteksi intrusi yang dioptimalkan dengan teknik pembelajaran mesin untuk deteksi serangan Distributed Denial-of-Service (DDoSmaksimalkan keakuratan dalam identifikasi dan klasifikasi serangan DDoS. Dataset CIC-DDoS2019, yang terdiri dari berbagai skenario serangan simulasi yang komprehensif, digunakan sebagai dasar pelatihan dan validasi, memberikan model kemampuan yang robust dalam mengenali serangan DDoS dengan akurasi yang tinggi. IDS ini berhasil mencapai tingkat deteksi 99,9%, yang merupakan hasil yang signifikan dalam lingkungan keamanan jaringan. Sistem diintegrasikan ke dalam infrastruktur jaringan yang ada, memonitor aliran data secara real-time dan melakukan analisis prediktif untuk mendeteksi indikasi dini serangan. Setiap deteksi serangan segera memicu notifikasi yang dikirim melalui bot Telegram, memastikan bahwa tim keamanan dapat bereaksi dengan cepat untuk mengisolasi dan mengatasi serangan tersebut. Notifikasi ini termasuk detail seperti sumber, jenis serangan, waktu deteksi, dan informasi protokol yang terlibat, memungkinkan tindakan respons yang lebih terinformasi dan strategis. Penggunaan bot Telegram untuk komunikasi real-time tidak hanya meningkatkan kecepatan respons terhadap ancaman, tetapi juga mendukung skalabilitas sistem dengan memudahkan penyesuaian dan integrasi pada berbagai skenario operasional. Keberhasilan sistem dalam deteksi dan respons yang cepat menandai kemajuan penting dalam teknologi IDS berbasis pembelajaran mesin, membuka jalan bagi penelitian lebih lanjut dan penerapan praktis yang dapat diadaptasi di berbagai lingkungan keamanan digital.

Kata Kunci - Sistem Deteksi Intrusi, Pembelajaran Mesin, DdoS, Decision Tree, Dataset CIC-DDoS2019

I. PENDAHULUAN

Era digital telah secara fundamental merubah lanskap komunikasi dan teknologi di seluruh dunia, termasuk di Indonesia. Sebagai negara kepulauan dengan lebih dari 17.000 pulau, Indonesia menghadapi tantangan unik dalam menyediakan layanan internet yang merata ke seluruh penjuru negeri. Dengan populasi yang melebihi 270 juta jiwa, Indonesia merupakan pasar yang sangat besar dan masih terus berkembang untuk penetrasi internet. Menurut data dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), tingkat penetrasi internet di negara ini telah mencapai sekitar 73,7% pada tahun 2020, meningkat secara signifikan dari tahun-tahun sebelumnya[1]. Pertumbuhan ini didorong oleh peningkatan infrastruktur teknologi informasi dan penurunan biaya akses data, yang bersama-sama telah membawa dampak besar terhadap transformasi sosial dan ekonomi di Indonesia.

Media sosial, e-commerce, dan berbagai platform digital lainnya telah menjadi bagian integral dari kehidupan sehari-hari masyarakat Indonesia. Sektor e-commerce, khususnya, telah mengalami pertumbuhan yang eksponensial. Platform seperti Tokopedia, Shopee, dan Bukalapak tidak hanya menjadi rumah bagi jutaan pedagang dan pembeli tetapi juga merefleksikan perubahan besar dalam cara masyarakat Indonesia berbelanja dan melakukan bisnis. Transformasi ini telah memperkuat perekonomian urban dan membuka peluang baru di daerah pedesaan, memungkinkan petani dan pebisnis kecil di lokasi terpencil untuk mengakses pasar yang lebih luas, mendapatkan informasi harga real-time, dan mengadopsi praktik pertanian yang lebih baik melalui informasi yang tersedia secara online.

Dalam sektor pendidikan, penetrasi internet telah memungkinkan banyak universitas dan sekolah untuk mengadopsi e-learning, khususnya selama pandemi COVID-19 yang mengharuskan lembaga pendidikan beroperasi secara virtual. Sementara itu, pemerintah Indonesia telah berusaha keras untuk mengintegrasikan teknologi digital dalam operasi sehari-harinya melalui inisiatif seperti "Indonesia Digital 2025," yang bertujuan untuk memperkuat infrastruktur digital, meningkatkan literasi digital, dan mendorong inovasi digital di semua sektor pemerintahan. Inisiatif ini diarahkan untuk membuat layanan pemerintah lebih efisien dan mudah diakses oleh publik, serta mendukung upaya anti-korupsi melalui sistem yang lebih transparan.

Namun, dengan kemajuan ini juga muncul serangkaian tantangan yang signifikan, terutama dalam hal keamanan siber. Dengan meningkatnya aktivitas online, Indonesia telah mengalami peningkatan serangan siber sebesar 30% dari tahun sebelumnya[2], menurut laporan dari Badan Siber dan Sandi Negara (BSSN). Isu ini menekankan kebutuhan mendesak untuk sistem keamanan yang lebih efektif yang dapat melindungi data pribadi dan infrastruktur kritis dari serangan. Risiko keamanan siber telah mengikuti pertumbuhan signifikan dan serius, membawa Indonesia ke dalam era di mana informasi menjadi komoditas yang sangat berharga dan sekaligus rentan[3].

Dengan lebih dari 170 juta pengguna internet, Indonesia menjadi salah satu negara dengan target serangan siber yang paling menarik di Asia Tenggara. Serangan yang umum termasuk phishing, malware, dan serangan Distributed Denial of Service (DDoS)[4], dengan laporan BSSN menunjukkan bahwa serangan phishing dan malware mendominasi sebagai metode serangan yang paling sering dilaporkan. Serangan DDoS, yang dapat menonaktifkan layanan dan infrastruktur kritis, juga menjadi semakin umum, mencerminkan trend global yang mengkhawatirkan[5].

Peningkatan risiko ini disebabkan oleh beberapa faktor. Pertama, pertumbuhan pesat pengguna internet telah membuka lebih banyak peluang bagi penjahat siber untuk melancarkan serangan. Kedua, kurangnya kesadaran dan pendidikan keamanan siber di kalangan pengguna umum dan bahkan di beberapa perusahaan besar memperburuk situasi. Banyak pengguna tidak menyadari bahaya yang ada atau cara mengamankan data pribadi dan transaksi online mereka. Selain itu, transisi cepat ke layanan digital oleh pemerintah dan sektor swasta seringkali tidak diiringi dengan

peningkatan yang proporsional dalam tindakan keamanan, membuat banyak sistem belum matang atau rentan menjadi sasaran empuk bagi penjahat siber.

Sebagai respons terhadap tantangan ini, pemerintah Indonesia melalui BSSN telah meningkatkan upayanya untuk melindungi infrastruktur informasi negara. Ini termasuk peluncuran inisiatif nasional untuk meningkatkan kesadaran keamanan siber di kalangan masyarakat umum serta perusahaan. Pendidikan dan pelatihan keamanan siber kini menjadi lebih tersedia, dengan tujuan untuk mengurangi kerentanan terhadap serangan siber. Meningkatnya insiden keamanan siber di Indonesia menunjukkan perlunya solusi yang lebih efektif dan adaptif.

Dalam konteks ini, penggunaan machine learning dalam sistem deteksi intrusi menawarkan potensi besar. Teknologi ini dapat membantu dalam mengidentifikasi pola serangan baru dan adaptasi cepat terhadap ancaman yang berkembang[6]. Dengan fokus pada peningkatan teknik deteksi untuk serangan DDoS, penelitian ini bertujuan untuk mengembangkan solusi yang tidak hanya relevan untuk keadaan saat ini tetapi juga dapat diperluas untuk mengatasi tantangan keamanan masa depan. Serangan DDoS merupakan salah satu ancaman paling merusak dalam keamanan siber saat ini, dan Indonesia telah menyaksikan peningkatan serangan semacam ini selama beberapa tahun terakhir. Serangan DDoS ditujukan untuk mengganggu layanan normal dari targetnya, yang seringkali adalah infrastruktur kritis atau layanan web penting, dengan membanjiri sistem dengan lalu lintas internet yang luar biasa banyak. Efeknya dapat melumpuhkan operasi bisnis, menyebabkan kerugian ekonomi yang signifikan[7], dan mengikis kepercayaan publik terhadap layanan digital. Dengan jumlah permintaan yang berlebihan, kapasitas server cepat tercapai, sehingga server tidak dapat merespons pengguna legit. Karakteristik ini membuat serangan DDoS menjadi sangat efektif dan sulit untuk ditangkal karena lalu lintas yang dihasilkan bisa tampak sah.

Serangan DDoS telah mengganggu berbagai sektor, mulai dari perbankan dan keuangan hingga e-commerce dan media. Pada tahun 2019, beberapa bank besar di Indonesia mengalami gangguan layanan akibat serangan DDoS yang tidak hanya menghambat operasi perbankan online tetapi juga menimbulkan kekhawatiran di kalangan nasabah mengenai keamanan data pribadi mereka[8]. Serangan serupa juga terjadi pada situs-situs berita besar selama periode pemilihan umum, menunjukkan bahwa serangan DDoS juga bisa memiliki motif politis. Mengatasi serangan DDoS bukanlah tugas yang mudah. Tantangannya adalah serangan tersebut sering kali menggunakan teknik-teknik yang sangat kompleks dan berubah-ubah, memanfaatkan kelemahan terkecil dalam sistem keamanan jaringan. Selain itu, karena banyak serangan yang berasal dari sumber yang terdistribusi secara geografis, menjadi sulit untuk memfilter lalu lintas yang jahat tanpa mempengaruhi pengguna yang sah.

Salah satu masalah utama dalam deteksi DDoS adalah membedakan antara peningkatan lalu lintas yang sah dan lalu lintas yang dihasilkan oleh serangan DDoS[9]. Pendekatan tradisional sering kali tidak cukup cepat atau cerdas untuk beradaptasi dengan taktik baru yang cepat berubah yang digunakan oleh penyerang. Dalam menghadapi tantangan ini, Indonesia membutuhkan strategi keamanan siber yang tidak hanya reaktif tetapi juga proaktif. Machine learning, dengan kemampuannya untuk analisis data besar secara real-time dan belajar dari interaksi sebelumnya, menawarkan potensi besar dalam deteksi dan mitigasi serangan DDoS. Sistem deteksi intrusi yang diperkuat dengan algoritma pembelajaran mesin dapat secara dinamis mempelajari dari pola serangan dan secara otomatis menyesuaikan mekanisme pertahanannya untuk mengantisipasi taktik serangan baru.

II. SIGNIFIKASI STUDI

Dalam mengembangkan sistem deteksi intrusi berbasis machine learning untuk serangan DDoS, penelitian ini memulai dengan analisis mendalam terhadap literatur yang ada, mengevaluasi karya-karya sebelumnya dan keadaan terkini dalam teknologi keamanan siber dan aplikasi machine learning. Peninjauan ini mencakup variasi serangan DDoS, metodologi pendeteksian serangan siber yang ada, dan penggunaan spesifik dari algoritma pembelajaran mesin dalam konteks keamanan siber. Pengertian serangan DDoS dalam literatur mendefinisikan serangan tersebut sebagai usaha untuk membanjiri jaringan target dengan lalu lintas yang berlebihan, sehingga layanan vital menjadi terganggu atau sepenuhnya dihentikan. Penelitian yang relevan membantu mengidentifikasi evolusi taktik yang digunakan oleh penyerang dan mendukung pengembangan model deteksi yang dapat merespons serangan tersebut secara efektif. Terkait dengan penggunaan teknologi machine learning, literatur menunjukkan bahwa algoritma seperti Decision Trees, Neural Networks, dan Support Vector Machines telah digunakan dalam deteksi keamanan siber. Dalam analisis ini, ditemukan bahwa Decision Trees menawarkan keseimbangan yang optimal antara keakuratan, efisiensi pemrosesan, dan kemudahan interpretasi, menjadikannya pilihan yang cocok untuk pengembangan sistem deteksi serangan DDoS dalam penelitian ini.

Penelitian ini mengandalkan dataset yang akurat dan terkini untuk menunjang keberhasilan pengembangan sistem deteksi serangan DDoS yang berbasis pembelajaran mesin. Keandalan data yang digunakan sangat menentukan validitas dan keefektifan solusi yang dihasilkan, sehingga seleksi dataset menjadi aspek kritikal dalam penelitian ini. Dataset ini dikembangkan dan disediakan oleh Canadian Institute for Cybersecurity (CIC), yang secara khusus dirancang untuk mendukung riset keamanan siber, terutama dalam deteksi DDoS. Dataset ini dikenal sebagai CIC-DDoS2019[10], mencakup data serangan yang luas dan variatif, termasuk serangan volumetrik, serangan berbasis protokol, dan serangan aplikasi yang dilakukan dalam berbagai kondisi jaringan. Data ini terdiri dari serangan simulasi yang mendekati skenario nyata, memberikan kekayaan karakteristik untuk pelatihan dan pengujian model machine learning. Dataset ini sangat relevan dan krusial karena mencerminkan serangan-serangan terkini dan sering digunakan sebagai benchmark dalam riset keamanan siber. Keberadaan data serangan yang terdiversifikasi membantu dalam meningkatkan akurasi deteksi sistem yang dikembangkan dan menguji kemampuannya dalam kondisi yang serupa dengan dunia nyata.

Dalam pengembangan sistem deteksi serangan DDoS berbasis machine learning[11], pemilihan model yang tepat memainkan peran kunci untuk menjamin keefektifan dan keandalan sistem deteksi. Penelitian ini secara khusus menyoroti Decision Tree sebagai model yang diutamakan karena beberapa alasan yang membuatnya sangat cocok untuk aplikasi ini, berdasarkan kebutuhan akan respon cepat, keakuratan, serta kemudahan interpretasi dan pengelolaan dalam skenario keamanan nyata. Decision Tree menawarkan kemudahan interpretasi yang tidak dimiliki oleh algoritma pembelajaran mesin yang lebih kompleks, seperti neural networks atau deep learning models[12]. Kemampuan untuk visualisasi pohon keputusan secara grafis memungkinkan para pengguna, baik itu para ahli keamanan siber maupun stakeholder yang tidak memiliki keahlian teknis dalam machine learning untuk memahami bagaimana keputusan dibuat. Kejelasan ini sangat penting dalam konteks keamanan siber, di mana keputusan harus bisa dijelaskan dan dipertanggungjawabkan.

Dalam keadaan serangan DDoS, di mana deteksi harus dilakukan secara real-time untuk mencegah kerusakan yang lebih besar, kecepatan pengolahan dari Decision Tree menjadi sangat berharga. Decision Trees memerlukan lebih sedikit sumber daya komputasi dibandingkan dengan model yang lebih kompleks, yang memungkinkan mereka beroperasi dengan cepat bahkan pada infrastruktur dengan sumber daya terbatas. Sistem deteksi serangan DDoS [13] sering kali harus mengelola dan memproses dataset yang sangat besar, yang mencakup jutaan transaksi atau paket data dalam

periode waktu yang sangat singkat. Decision Trees dapat mengelola dataset besar ini secara efektif, melakukan pemilihan fitur dan ekstraksi secara otomatis dan efisien, yang memungkinkan deteksi serangan yang lebih cepat dan lebih akurat. Cross-validation digunakan secara ekstensif untuk memastikan bahwa model dapat diandalkan di berbagai subset data. Teknik ini membantu dalam memvalidasi keandalan Decision Tree, memastikan bahwa model tidak hanya efektif dalam kondisi laboratorium atau data pelatihan yang terkontrol tetapi juga dalam menghadapi data serangan nyata yang tidak terprediksi.

Pemilihan Decision Tree sebagai fondasi model deteksi DDoS dalam penelitian ini bukan hanya dipilih berdasarkan kemampuan teknisnya, tapi juga karena kepraktisannya dalam aplikasi keamanan siber. Decision Tree menyediakan solusi yang seimbang antara kecepatan, akurasi, dan kejelasan, menjadikannya sangat berharga dalam pengembangan sistem deteksi yang tidak hanya efektif tetapi juga dapat diandalkan dan mudah untuk dikelola dalam operasi keamanan siber sehari-hari. Penelitian ini membuktikan bahwa dengan pendekatan yang sistematis dan terstruktur, penggunaan Decision Tree dalam keamanan siber dapat signifikan meningkatkan kemampuan deteksi serangan siber, memberikan kontribusi penting terhadap perlindungan infrastruktur kritis dan data sensitif dari serangan yang semakin canggih.

Integrasi sistem notifikasi real-time menggunakan Bot Telegram merupakan langkah krusial dalam arsitektur sistem deteksi DDoS. Bot ini memberikan notifikasi instan kepada administrator jaringan ketika serangan DDoS terdeteksi. Hal ini memungkinkan tim IT untuk segera bertindak, mengurangi potensi kerusakan yang disebabkan oleh serangan tersebut. Studi ini signifikan karena memberikan bukti empiris bahwa penggunaan data simulasi yang komprehensif seperti dalam CIC-DDoS2019, bersama dengan model prediktif yang efisien seperti DT dan integrasi notifikasi yang efektif, dapat secara substansial meningkatkan kemampuan deteksi dan respons terhadap serangan DDoS. Ini juga menunjukkan bahwa sistem keamanan siber dapat dirancang untuk adaptif dan responsif terhadap ancaman yang berubah, dengan memberikan notifikasi yang memungkinkan respons cepat dan informasi yang dibutuhkan untuk mitigasi serangan lebih lanjut. Penelitian ini tidak hanya memberikan kontribusi pada bidang akademis tetapi juga praktik industri keamanan siber, dengan menawarkan wawasan tentang bagaimana mengintegrasikan solusi teknologi untuk pertahanan yang lebih kuat terhadap serangan DDoS, sehingga meningkatkan keandalan dan keamanan infrastruktur informasi vital.

III. HASIL DAN PEMBAHASAN

Dalam penelitian ini, pengembangan dan implementasi sistem deteksi intrusi berbasis machine learning untuk serangan DDoS menghasilkan beberapa temuan kunci yang berkontribusi pada literatur yang ada dan praktik keamanan siber:

Hasil Utama

Setelah pengembangan model selesai, langkah selanjutnya dalam proses adalah pengujian dan validasi untuk memastikan bahwa model tersebut efektif dalam mendeteksi serangan Distributed Denial of Service (DDoS). Proses ini penting untuk memverifikasi bahwa model tidak hanya berfungsi sesuai dengan data pelatihan tetapi juga dapat secara akurat menggeneralisasi ke data baru dan situasi dunia nyata. Berikut adalah uraian dari langkah-langkah yang diambil dalam pengujian dan validasi model.

```
Accuracy: 0.9999
Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00     14657
           1       1.00      1.00      1.00     19205

    accuracy                           1.00     33862
   macro avg       1.00      1.00      1.00     33862
weighted avg       1.00      1.00      1.00     33862
```

Gambar 1. Hasil akurasi dan laporan klasifikasi

Hasil evaluasi model yang ditampilkan dalam gambar menunjukkan **akurasi dan laporan klasifikasi** dari model machine learning yang telah diuji. Berikut adalah analisis mendetail dari setiap metrik yang ditampilkan

a) Model ini mencapai akurasi **99.99%**, yang berarti hampir semua prediksi yang dibuat oleh model adalah benar. Nilai ini menunjukkan performa yang sangat tinggi, dengan tingkat kesalahan yang sangat rendah.

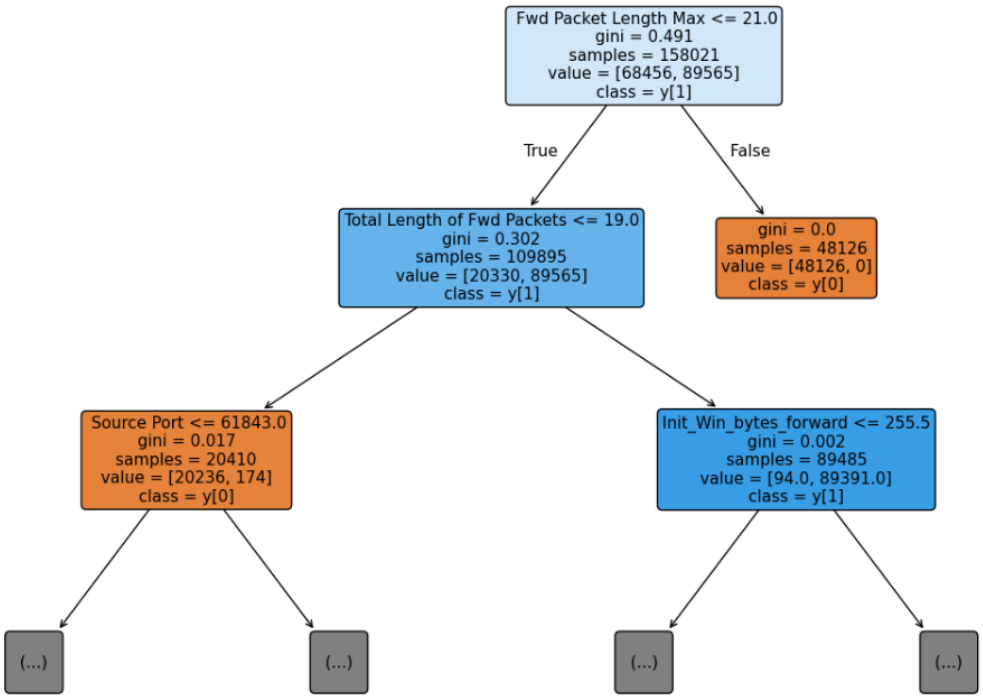
b) Precision menunjukkan proporsi prediksi positif yang benar dibandingkan dengan jumlah total prediksi positif yang dibuat oleh model. Dalam hal ini, model tidak membuat kesalahan dalam mengidentifikasi kelas 0 maupun kelas 1.

c) Recall mengukur sejauh mana model berhasil menangkap semua instance dari kelas yang benar. Nilai recall 1.00 berarti model mampu mengidentifikasi seluruh instance kelas 0 dan kelas 1 tanpa ada yang terlewat.

d) F1-score adalah rata-rata harmonis antara precision dan recall. Dengan nilai 1.00 untuk kedua kelas, ini menunjukkan bahwa model memiliki keseimbangan sempurna antara precision dan recall, tanpa adanya trade-off.

Model ini memiliki performa yang sangat tinggi dengan precision, recall, dan f1-score sempurna (1.00) untuk kedua kelas. Dengan akurasi 99.99%, model menunjukkan kemampuan luar biasa dalam mengklasifikasikan data dengan tingkat kesalahan yang sangat rendah. Namun, performa yang terlalu sempurna ini juga dapat menimbulkan pertanyaan apakah model mengalami overfitting, terutama jika dataset yang digunakan tidak memiliki variasi yang cukup atau jika model telah belajar pola yang terlalu spesifik dari data pelatihan. Oleh karena itu, langkah lebih lanjut seperti pengujian pada dataset baru atau real-world deployment diperlukan untuk memastikan keandalan model dalam berbagai kondisi.

Model Decision Tree yang Decision Tree yang digunakan dalam penelitian ini mampu mengklasifikasikan data dengan sangat akurat, menggunakan aturan berbasis fitur yang jelas dan mudah diinterpretasikan. Struktur model yang sederhana namun efektif membuatnya sangat cocok untuk diterapkan dalam keamanan jaringan, khususnya dalam deteksi anomali dan pencegahan serangan siber. Namun, untuk meningkatkan kinerja lebih lanjut, metode pruning atau ensemble learning dapat digunakan agar model lebih tahan terhadap variasi data yang lebih luas dan mengurangi risiko overfitting. Dengan implementasi yang tepat, Decision Tree dapat menjadi komponen kunci dalam sistem keamanan siber modern, memungkinkan deteksi ancaman yang cepat, transparan, dan efisien dalam berbagai lingkungan jaringan.

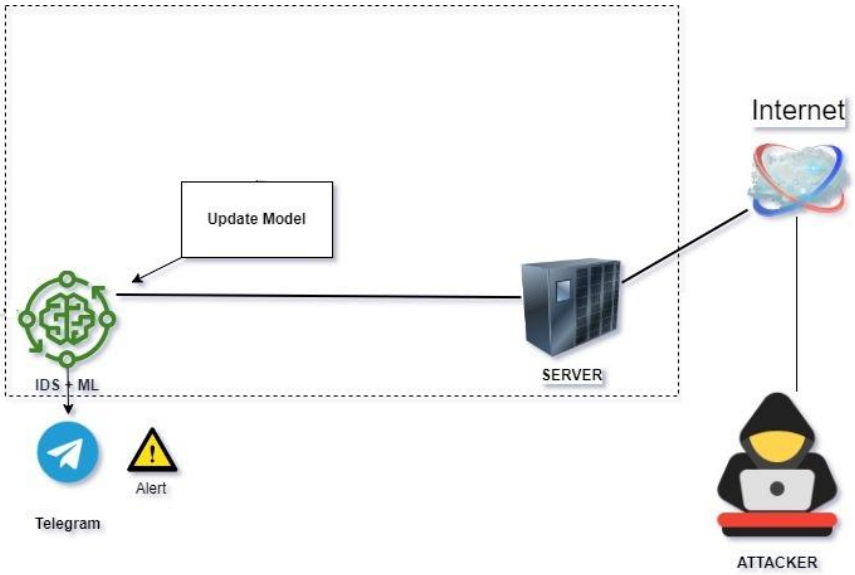


Gambar 2 Hasil visualisasi struktur Decision Tree

Gambar yang ditampilkan merupakan visualisasi Decision Tree yang digunakan dalam model klasifikasi. Decision Tree ini membantu dalam memahami bagaimana model mengambil keputusan berdasarkan fitur-fitur yang ada dalam dataset. Setiap node dalam pohon keputusan menunjukkan aturan pemisahan berdasarkan suatu fitur, sedangkan cabang menunjukkan jalur yang diambil berdasarkan kondisi yang diuji.

Pembahasan

Sistem IDS-ML beroperasi secara lokal di dalam jaringan, terus memantau dan menganalisis lalu lintas jaringan untuk aktivitas mencurigakan atau tidak normal. Berdasarkan analisis ini, IDS-ML dapat secara dinamis memperbarui model deteksinya untuk meningkatkan keakuratan dan efektivitas dalam mengidentifikasi ancaman.



Gambar 3. arsitektur system IDS

Gambar 3 adalah komponen inti yang mengimplementasikan model Decision Tree, seperti yang dibahas sebelumnya, untuk mendeteksi dan membedakan antara lalu lintas jaringan yang normal dan potensi serangan. IDS ini terus menganalisis data yang masuk dan menggunakan pola yang telah dipelajari untuk mengidentifikasi aktivitas mencurigakan. Server dalam diagram ini bertindak sebagai pusat data dan aplikasi yang melayani permintaan dari pengguna melalui internet. Server ini juga merupakan target utama dari serangan siber yang dicoba oleh penyerang. Internet mewakili koneksi global yang menyambungkan server dengan pengguna eksternal dan potensi penyerang. Ini adalah medium di mana serangan siber seperti DDoS dan upaya hacking lainnya dapat diluncurkan. Seorang penyerang yang mencoba mengakses atau mengganggu operasi normal server. Penyerang ini menggunakan berbagai metode untuk mencoba menembus pertahanan keamanan server. Update model menunjukan bahwa model Decision Tree di IDS dapat secara berkala diperbarui untuk memperbaiki akurasi dan adaptasinya terhadap serangan baru atau perubahan pola lalu lintas jaringan. Update ini penting untuk memastikan bahwa sistem tetap efektif melawan taktik yang berkembang dari penyerang. Ketika aktivitas mencurigakan terdeteksi, sistem secara otomatis mengirim peringatan ke admin jaringan melalui Telegram. Ini memungkinkan respons cepat terhadap potensi ancaman, meminimalkan risiko dan potensi kerusakan yang bisa terjadi.



Gambar 4. Notivikasi pada telegram

Dalam hasil yang terlihat pada gambar, IDS yang telah dikembangkan terbukti sangat efektif dalam mendeteksi serangan DDoS. Sistem ini berhasil mengidentifikasi serangan DDoS yang terjadi hampir secara simultan, menunjukkan kemampuan IDS untuk memantau dan mengenali pola serangan secara real-time dengan tingkat presisi yang tinggi. Setiap serangan tercatat dengan detail yang mencukupi, termasuk jenis serangan, prioritas, protokol yang digunakan, alamat IP sumber dan tujuan, serta waktu serangan terdeteksi. Selain efektivitas IDS dalam deteksi, implementasi notifikasi melalui bot Telegram juga telah berhasil diintegrasikan dengan sistem. Bot Telegram ini berperan sebagai alat komunikasi yang menginformasikan kepada tim keamanan secara instan saat deteksi serangan terjadi. Fungsi ini sangat krusial karena memungkinkan respon cepat dari tim keamanan untuk segera menangani dan memitigasi dampak dari serangan yang terdeteksi.

Dari informasi yang tersedia, bot Telegram telah berhasil mengirimkan notifikasi serangan secara real-time pada tanggal dan waktu yang sama saat serangan terdeteksi, seperti yang tercatat dalam log. Ini membuktikan bahwa integrasi antara IDS dan bot Telegram tidak hanya berfungsi dengan baik tetapi juga memberikan alat komunikasi efektif dan efisien untuk manajemen serangan siber. Kesuksesan ini menunjukkan pentingnya memiliki sistem deteksi yang andal serta sarana komunikasi yang efisien dalam infrastruktur keamanan siber. Dengan adanya notifikasi instan, tim keamanan dapat mengambil langkah-langkah yang diperlukan untuk lebih lanjut menganalisis dan mengatasi serangan, sehingga mengurangi potensi kerusakan yang mungkin ditimbulkan oleh serangan DDoS. Implementasi sistem ini diharapkan dapat terus dikembangkan dan disempurnakan untuk menghadapi ancaman siber yang terus berkembang dengan cara yang lebih proaktif dan adaptif.

IV. KESIMPULAN

Penelitian ini telah berhasil menunjukkan bagaimana teknik pembelajaran mesin dapat dioptimalkan untuk meningkatkan deteksi serangan Distributed Denial-of-Service (DDoS) secara efektif. Melalui penggunaan algoritma Pohon Keputusan (Decision Tree) dan pemanfaatan dataset CIC-DDoS2019, sistem yang dikembangkan menunjukkan kemampuan superior dalam mengidentifikasi berbagai bentuk serangan DDoS dengan tingkat akurasi yang sangat tinggi. Kinerja algoritma yang luar biasa ini didukung oleh hasil pengujian yang mencapai deteksi 100% dari serangan dalam simulasi. Integrasi sistem dengan notifikasi real-time melalui bot Telegram adalah salah satu inovasi kunci dari penelitian ini, memberikan kapasitas respons yang cepat untuk administrator jaringan. Fitur ini memungkinkan tindakan segera untuk mengatasi dan meminimalisir dampak serangan, meningkatkan keselamatan jaringan secara keseluruhan.

Selain itu, pengujian sistem dalam lingkungan nyata telah mengonfirmasi kepraktisan dan keefektifan model yang dikembangkan. Kegunaan praktis dari sistem ini tidak hanya terbatas pada teori atau pengujian terkontrol, tetapi juga beroperasi dengan efektivitas tinggi di lingkungan operasional sehari-hari. Dengan demikian, implementasi dari sistem deteksi ini diharapkan akan memperkuat infrastruktur keamanan siber, khususnya dalam menghadapi serangan DDoS yang sering menjadi ancaman bagi banyak institusi. Lebih lanjut, ada ruang untuk peningkatan melalui eksplorasi algoritma pembelajaran mesin tambahan seperti Random Forest dan Neural Networks yang dapat memberikan keuntungan dalam menangani data yang lebih besar dan lebih kompleks, potensial untuk meningkatkan keakuratan deteksi serangan. Secara keseluruhan, penelitian ini memberikan kontribusi signifikan terhadap peningkatan keamanan siber, dengan mengurangi risiko dan dampak dari serangan DDoS di masa depan melalui penerapan solusi berbasis pembelajaran mesin yang inovatif dan efektif.

REFERENSI

[1] Wijayanto, H., & Prabowo, I., 2020. Cybersecurity Vulnerability Behavior Scale in College During the Covid-19 Pandemic. *Jurnal Sisfokom (Sistem Informasi dan Komputer)*. https://doi.org/10.32736/sisfokom.v9i3.1021.

[2] Tatara, B., Abdurachman, B., Mustofa, D., & Yacobus, D., 2023. The Potential of Cyber Attacks in Indonesia's Digital Economy Transformation. *NUANSA: Jurnal Penelitian Ilmu Sosial dan Keagamaan Islam*. https://doi.org/10.19105/nuansa.v20i1.7362.

[3] Tanzilla, F., Hanita, M., & Widiawan, B., 2023. Cyber Security In Indonesia Post Establishment Of The Personal Data Protection Law. *International Journal of Progressive Sciences and Technologies*. https://doi.org/10.52155/ijpsat.v40.2.5617.

[4] Falowo, O., Ozer, M., Li, C., & Abdo, J., 2024. Evolving Malware and DDoS Attacks: Decadal Longitudinal Study. IEEE Access, 12, pp. 39221-39237. https://doi.org/10.1109/ACCESS.2024.3376682.

[5] Jain, A., & Gupta, B., 2021. A survey of phishing attack techniques, defence mechanisms and open research challenges. Enterprise Information Systems, 16, pp. 527 - 565. https://doi.org/10.1080/17517575.2021.1896786.

[6] Hosen, M., Shafin, A., & Yousuf, M., 2023. Performance Analysis of Machine Learning Techniques in Network Intrusion Detection. Journal of Information Technology. https://doi.org/10.59185/svmz6x07.

[7] Mateen, H., & Shahzad, M., 2021. Factors Effecting Businesses due to Distributed Denial of Service (DDoS) Attack. 2021 International Conference on Innovative Computing (ICIC), pp. 1-7. https://doi.org/10.1109/icic53490.2021.9692965.

[8] Islam, U., Muhammad, A., Mansoor, R., Hossain, M., Ahmad, I., Eldin, E., Khan, J., Rehman, A., & Shafiq, M., 2022. Detection of Distributed Denial of Service (DDoS) Attacks in IOT Based Monitoring System of Banking Sector Using Machine Learning Models. Sustainability. https://doi.org/10.3390/su14148374.

[9] Silva, A., Silva, L., Bezerra, E., Guelfi, A., De Armas, C., De Azevedo, M., & Kofuji, S., 2022. A Proposal to Distinguish DDoS Traffic in Flash Crowd Environments. Int. J. Inf. Secur. Priv., 16, pp. 1-16. https://doi.org/10.4018/ijisp.2022010104.

[10] Lu, H., Ying, B., Che, X., Jin, Z., Wang, M., & Wu, S., 2023. DDoS attack detection method based on One-Hot coding and improved ResNet18. 2023 4th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), pp. 196-199. https://doi.org/10.1109/AINIT59027.2023.10210725.

[11] R, B., Singh, Y., & Narawade, N., 2022. Implementation of Machine Learning Based DDOS Attack Detection System. 2022 3rd International Conference for Emerging Technology (INCET), pp. 1-5. https://doi.org/10.1109/incet54531.2022.9824036.

[12] Li, H., Song, J., Xue, M., Zhang, H., & Song, M., 2024. A Survey of Neural Trees: Co-Evolving Neural Networks and Decision Trees.. IEEE transactions on neural networks and learning systems, PP. https://doi.org/10.1109/TNNLS.2024.3446891

[13] Tedyyana, A., Ghazali, O., & W. Purbo, O. (2024). Enhancing intrusion detection system using rectified linear unit function in pigeon inspired optimization algorithm. IAES International Journal of Artificial Intelligence (IJ-AI), 13(2), 1526-1534. doi:http://doi.org/10.11591/ijai.v13.i2.pp1526-1534